

Administrator's Guide

Citrix NFuse™

Version 1.6

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Citrix Systems, Inc.

© 2000-2001 Citrix Systems, Inc. All rights reserved.

Citrix and ICA are registered trademarks, and MetaFrame, MetaFrame XP, Citrix Extranet, SecureICA, NFuse, VideoFrame, Program Neighborhood, Citrix Solutions Network, are trademarks of Citrix Systems, Inc. in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Sun, Java, Solaris, and SPARC are trademarks or registered trademarks of Sun Microsystems, Inc.

Macintosh and Mac are registered trademarks of Apple Computer, Inc.

Microsoft, Windows, Windows NT, MS-DOS, and ActiveX are registered trademarks of Microsoft Corporation.

Netscape Navigator is a registered trademark of Netscape Communications Corporation.

Linux is a registered trademark of Linus Torvalds.

AIX and OS/2 are registered trademarks of International Business Machines Corporation.

HP-UX is a registered trademark of Hewlett-Packard Company.

Novell Directory Services and NDS are registered trademarks of Novell, Inc. in the United States and other countries. Novell Client is a trademark of Novell, Inc.

Apache is either a registered trademark or trademark of the Apache Software Foundation in the United States and/or other countries.

JavaServer Pages and iPlanet Web Server are either registered trademarks or trademarks of Sun Microsystems Corporation in the United States and/or other countries.

RSA Encryption © 1996-1997 RSA Security Inc., All Rights Reserved.

This product incorporates IBM's XML Parser for C++ Edition and IBM's XML Parser for Java Edition, © 1999, 2000 IBM Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Document Code nfuse.admin.1.6.adm

Contents

Chapter 1 Before You Begin	5
Who Should Read this Guide	5
How to Use this Guide	5
Document Conventions	5
Finding More Information	6
Citrix Developer Network	7
Citrix on the World Wide Web	8
Reader Comments	8
Chapter 2 Welcome to Citrix NFuse	9
NFuse Features	9
New Features in NFuse 1.6	10
NFuse Components	11
Citrix Server Farm	12
Web Server	13
ICA Client Device	13
NFuse and the ICA Win32 Program Neighborhood Agent	14
How NFuse Works	15
System Requirements	16
Citrix Server Requirements	16
Supported MetaFrame Versions	16
Additional Software Requirements	17
General Configuration Requirements	17
Backward Compatibility	18
Web Server Requirements	18
ICA Client Device Requirements	20
Overview of this Manual	22
What to Do Next	22
Chapter 3 Configuring Your Web Server	23
Tasks to Complete	23
Web Server Extension Installation	23
Upgrading Existing NFuse Installations	24
Installing NFuse During MetaFrame XP Installation	24
Installing the Web Server Extension on Microsoft IIS	25

Plugging the Citrix XML Service into IIS	26
Installing the Web Server Extension on iPlanet Web Server and Apache Server	28
Configuring iPlanet Web Server	31
Configuring Apache Server	32
Configuring Web Server Extension Properties	34
Making NFuse Available to Users	41
What to Do Next	42
Chapter 4 Configuring ICA Client Devices	43
Tasks to Complete	43
Configuring Web-Based ICA Client Installation	43
ICA Client Installation Files	44
ICA Win32 Client Installation Files	45
Configuring Web Browsers	45
Configuring the ICA Java Client	46
Configuring the ICA Macintosh Client	48
What to Do Next	49
Chapter 5 Configuring NFuse Security	51
ICA Client Device — NFuse Web Server Communication	51
Risks	52
Recommendations	52
Implement SSL-Capable Web Servers and Web Browsers	52
NFuse Web Server — Citrix Server Communication	53
Risks	53
Recommendations	54
Use the Citrix SSL Relay	54
Running the NFuse Web Server on Your Citrix Server	56
ICA Client — Citrix Server Communication	57
Risks	57
Recommendations	57
Chapter 6 ICA Program Neighborhood Agent Configuration	59
Securing the Program Neighborhood Agent With SSL	64
Index	65

Convention	Meaning
...(ellipsis)	Indicates a command element can be repeated.
Monospace	Represents examples of screen text or entries that you might type at the command line or initialization files.
Code Sample	Example code appears in front of a gray background, as in the example below: <pre><html > <body></body> </html ></pre>
▶	Indicates a procedure with sequential steps.
•	Indicates a list of related information, not procedural steps.

Finding More Information

NFuse includes the following documentation:

- The *Citrix NFuse Administrator's Guide* (this document) explains how to install and configure NFuse.
- The *Configuring NFuse* PDF file explains how to customize NFuse. This file is located on the NFuse CD-ROM as well as on the Citrix Web site (<http://www.citrix.com/support/>). Click the Product Documentation tab.
- The NFuse Readme file contains last minute updates, corrections to the documentation, and a list of known problems. This file is located on the NFuse CD-ROM as well as on the Citrix Web site (<http://www.citrix.com/support>). Click the Product Documentation tab.
- The Web-based ICA Client installation Readme file contains information on using the standalone Web-based installation package that is included on the NFuse CD-ROM and in the downloadable Web-based installation image on the Citrix download site. See the file Readme.htm in the NFuse CD-ROM's WebInst directory or in the downloaded CD image for information.
- The *Citrix MetaFrame XP for Windows, Version 1.0, Feature Release 1 Administrator's Guide* explains how to install and configure MetaFrame XP on Windows servers. Included in this documentation is information about publishing applications, configuring the Citrix XML Service, and configuring the Citrix SSL Relay. The *MetaFrame XP Administrator's Guide* is located on the MetaFrame XP CD-ROM.

- The *Feature Release 1 and Service Pack 3 Installation Guide for Citrix MetaFrame for Windows Version 1.8* tells administrators how to install and configure Service Pack 3 and Feature Release 1 on MetaFrame 1.8 for Windows servers. Included in this documentation is information about configuring the Citrix XML Service and the Citrix SSL Relay. The Installation Guide is available on the Feature Release 1/Service Pack 3 CD-ROM and on the Citrix download site.
- The *Citrix MetaFrame for UNIX Operating Systems, Feature Release 1 for Version 1.1, Administrator's Guide* tells administrators how to install and configure MetaFrame for UNIX. Included in this documentation is information about publishing applications and how to configure the XML Relay for UNIX. The *MetaFrame for UNIX Administrator's Guide* is available on the MetaFrame for UNIX, Feature Release 1 CD-ROM.

Citrix Developer Network

The Citrix Developer Network (CDN) is a Citrix program that extends the reach of Citrix application server technology to independent software vendors, independent hardware vendors, system integrators, ICA licensees, and corporate IT developers who want to incorporate Citrix server-based computing solutions into their products.

The Citrix Developer Network is a membership program with open enrollment. Through the new CDN Web site, Citrix provides access to developer tool kits, technical information, and test programs needed to successfully “design in” or add Citrix server-based computing compatibility to hardware and software. The CDN program offers software development kits (SDKs) and test kits, with an emphasis on delivering enabling technologies that promote technical relationships with Citrix.

Register for the Citrix Developer Network at the CDN Web site:

<http://www.citrix.com/cdn>

Citrix on the World Wide Web

The Citrix Web site, at <http://www.citrix.com>, offers a variety of information and services for Citrix customers and users. From the Citrix home page, you can access Citrix online Technical Support Services and other information designed to assist NFuse administrators, including the following:

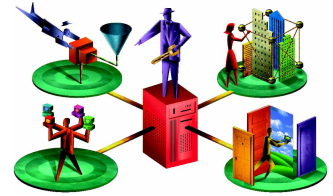
- Downloadable Citrix ICA Clients (available at <http://www.citrix.com/download>)
- Program information about Citrix Preferred Support Services options
- An FTP server containing the latest service packs, hotfixes, utilities, and product literature for download
- An online Solution Knowledgebase containing an extensive collection of technical articles, troubleshooting tips, and white papers
- Interactive online Solution Forums for discussion of technical issues with other users
- Frequently Asked Questions pages with answers to common technical and troubleshooting questions
- Citrix Documentation Library containing the latest MetaFrame documentation
- Information about programs and courseware for Citrix training and certifications
- Contact information for Citrix headquarters, including worldwide, European, Asia Pacific, and Japan headquarters

Reader Comments

It is our goal to provide you with accurate, clear, complete, and usable documentation for Citrix products. If you have any comments, corrections, or suggestions for improving our documentation, we would be happy to hear from you.

You can send e-mail to the authors at documentation@citrix.com. Please include the product name and version number, and the title of the document in your message.

Welcome to Citrix NFuse



Welcome to NFuse, a Web-based application deployment system from Citrix Systems, Inc. NFuse leverages the centralized application management capabilities of Citrix server software with new techniques for Web application deployment, resulting in a customizable Web-based application delivery mechanism. Using NFuse, you can create standalone Web sites for application access or Web sites that can be integrated into your corporate portal.

NFuse brings a powerful user interface to the application deployment process. This interface uses Java object technology executed on a Web server to dynamically create an HTML-based depiction of the Citrix server farm for each of your users. Included in each user's presentation are all of the applications published in the Citrix server farm for that user.

NFuse is a Web master's application, placing complete control over the application deployment process in the hands of the administrator.

NFuse Features

A Web interface for Citrix Program Neighborhood. Users of almost any ICA Client can benefit from the simplified application access provided by Program Neighborhood.

Complete administrative control over application deployment. Web server-side scripting lets you configure all ICA Client options in server-side scripts and ICA files.

Integration with popular Web technologies. NFuse's Java objects can be accessed from Web server scripts, such as Microsoft's Active Server Pages and Sun Microsystems' JavaServer Pages.

Secure Sockets Layer (SSL) support. NFuse supports SSL to secure communication between your Web server and Citrix server farm. SSL is an open, nonproprietary protocol that provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. SSL support is provided by enhancements to the NFuse Java objects and requires use of the Citrix SSL Relay in your server farm. Implementing SSL on your Web server together with Web browsers that support SSL ensures the security of data as it travels through your network.

Support for MetaFrame for UNIX Operating Systems. NFuse can deliver UNIX applications to your users. Support for MetaFrame for UNIX Operating System server farms allows NFuse to display and launch UNIX applications on your client devices.

Ticketing. This feature provides enhanced authentication security. NFuse can create tickets that authenticate users to Citrix applications. Tickets have a configurable expiration period and are valid for a single logon. After use, or after expiration, a ticket is invalid and cannot be used to access applications. Use of ticketing eliminates the explicit inclusion of credentials in the ICA files NFuse uses to launch applications.

Encrypted cookie data. Encrypting cookie data prevents passwords from being copied from client-side cookies.

Backup MetaFrame servers. Should the default MetaFrame server fail to respond to an NFuse request, the NFuse Web server sends the request to each of the servers in the backup list until one responds. Configuring backup MetaFrame servers ensures that users still have access to their applications in the event of a server failure.

Web-based ICA Client installation. You can also use NFuse to deploy ICA Clients to any device that has a Web browser. When a client device user visits an NFuse Web site, the Web-based ICA Client installation code detects the device and Web browser types and prompts the user to install an appropriate ICA Client. In addition, this NFuse release includes support for a Web-based installation mechanism that is independent of NFuse. You can use this independent Web-based installation mechanism to perform general deployment separate from your NFuse sites.

New Features in NFuse 1.6

Launching of published content. NFuse supports the new content publishing features of Feature Release 1 for MetaFrame XP.

NDS support. There is a separate NFuse Login page for NDS containing an context field and the ability for users to search for their user name in the tree to determine which context they are in.

ICA Win32 Program Neighborhood Agent support. The ICA Win32 Program Neighborhood Agent allows your users to access NFuse-enabled published applications directly from the Windows desktop without using a Web browser. You can remotely configure the placement of links to remote applications in the Start menu, on the Windows desktop, or in the Windows system tray. The Program Neighborhood Agent user interface can also be “locked down” to prevent user misconfiguration.

Guest users. This feature allows users to log in using a guest or anonymous account.

Logout button. This feature allows the user to log off, clear session cookies, and return to the NFuse Login page.

Improved client detection/installation. NFuse has improved client detection abilities and gives administrators more control over the installation options presented to users.

Help links. On-line help on every NFuse Web page for users to seek assistance.

Internet Server Application Program Interface (ISAPI) extension. The Citrix XML Service now contains an ISAPI extension that you can plug into Internet Information Server. Plugging the XML Service into IIS allows IIS to handle NFuse requests and serve NFuse Web pages on a shared TCP/IP port. This configuration frees you from having to dedicate a port to the XML Service and is useful in environments that do not permit opening additional TCP/IP ports on firewalls.

Active Directory and User Principal Name (UPN) support. All NFuse components are compatible with Microsoft Active Directory. Users visiting NFuse Web pages can log into a Citrix server farm that is part of an Active Directory deployment and seamlessly access Citrix published applications. The logon pages in NFuse Web sites are now compatible with Active Directory’s use of User Principal Names.

NFuse Components

An NFuse deployment involves the interaction of three network components:

- A Citrix server farm
- A Web server
- A client device with a Web browser and ICA Client

Citrix Server Farm

A Citrix *server farm* is a group of Citrix servers managed as a single entity. A server farm is composed of a number of MetaFrame servers operating together to serve applications to ICA Client users. Citrix supports farms composed of MetaFrame for Windows servers and farms composed of MetaFrame for UNIX Operating Systems servers.

Important among a server farm's standard capabilities is *application publishing*. This is an administrative task that lets Citrix server administrators make available to users specific applications hosted by the server farm. When a Citrix server administrator publishes an application for a group of users, that application becomes available as an object to which ICA Clients can connect and initiate ICA sessions.

The ICA Program Neighborhood Client interface automates the client-side configuration process by eliminating the need for administrators or ICA Client users to browse the network for published applications. Using Program Neighborhood, users can log in to the farm and receive a customized list of applications published for their individual user name. This list of applications is called an *application set*.

In an NFuse system, the NFuse Web server functions as a Web-based Program Neighborhood interface for connecting to a Citrix server farm. The NFuse Web server queries the MetaFrame server farm for application set information and then formats the results into HTML pages that a user can view in a Web browser.

To communicate with the Citrix server farm, the NFuse Web server communicates with the Citrix XML Service running on one or more MetaFrame servers. The *Citrix XML Service* is a MetaFrame component that provides published application information to ICA Clients and NFuse Web servers using TCP/IP. This service functions as the contact point between the server farm and NFuse's Web server component. The Citrix XML Service is installed with MetaFrame XP on MetaFrame XP for Windows systems, Citrix MetaFrame 1.8 Service Pack 2 on MetaFrame 1.8 for Windows systems, and Citrix MetaFrame 1.1 Feature Release 1 for UNIX Operating Systems on UNIX systems.

Web Server

The Web server in an NFuse system hosts the NFuse Java objects and Web server-side scripts. The NFuse Java objects provide the following services:

- Authenticate users to a Citrix server farm
- Retrieve application information, including a list of applications a user can access
- Give administrators the ability to modify the properties of individual applications before presenting them to users

NFuse Java objects are added to your Web server during NFuse installation. This installation program also adds Web pages and configuration files.

ICA Client Device

In the context of NFuse, an *ICA Client device* is any computing appliance capable of executing an ICA Client and a Web browser. ICA Client devices include desktop PCs and network computers, among others.

In an ICA Client device, the Web browser and ICA Client work together as a viewer and engine. The Web browser lets users view application sets (created by server-side scripting on the NFuse Web server) while the ICA Client acts as the engine that launches published applications.

NFuse is integrated with Web-based ICA Client installation. *Web-based ICA Client installation* is a Web browser-based method of deploying ICA Clients. When a client device user visits an NFuse Web site, the Web-based ICA Client installation code detects the device and Web browser types and prompts the user to install an appropriate ICA Client. In the case of 16- and 32-bit Windows devices, Web-based ICA Client installation can also detect the presence or absence of an installed ICA Client and prompt the user only if necessary. See “Configuring Web-Based ICA Client Installation” on page 43 for more information.

NFuse supports many Web browser/ICA Client combinations. For a complete list of supported browser/client combinations, see “ICA Client Device Requirements” on page 20.

NFuse and the ICA Win32 Program Neighborhood Agent

The ICA Win32 Program Neighborhood Agent allows users to access published applications using a Web browser. With the Program Neighborhood Agent, links to NFuse-enabled published applications appear in the user's Start menu, on the Windows desktop, or in the Windows system tray. Published applications appear to the user as locally accessible applications.

The Program Neighborhood Agent supports the following:

- “Locking-down” the client user interface
- Automatically refreshing application icons
- Pass-through authentication
- Secure Sockets Layer

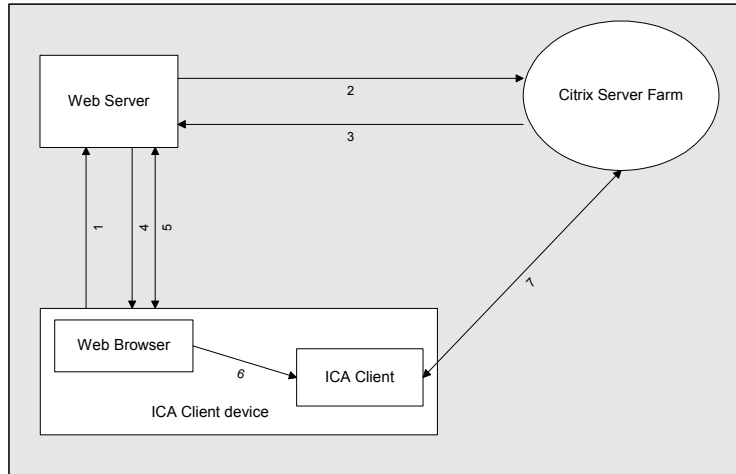
Configuration settings for the Program Neighborhood Agent are stored in a configuration file placed on the NFuse server when you install NFuse version 1.6. Application configuration information passed to the Program Neighborhood Agent using XML, allowing you to control connections and application sets from a central location. XML can pass through firewalls using port 80.

You can modify this configuration file to prevent users from editing certain settings and to “push” specific Program Neighborhood Agent settings to the client device. See chapter 6, “ICA Program Neighborhood Agent Configuration” on page 59.

For information about installing and using the Program Neighborhood Agent, see the *ICA Win32 Clients Administrator's Guide*, located in the \Doc directory of the ICA Client CD.

How NFuse Works

This diagram describes the interaction between the Citrix server farm, an NFuse Web server, and an ICA Client device.



1. An ICA Client device user uses a Web browser to view the NFuse Login page and enters their user credentials. The credentials are sent as a standard HTTP request over the default HTTP port 80.
2. The Web server reads the user's information and uses the NFuse Java objects to forward the information to the Citrix XML Service on a Citrix server in the server farm. The designated server acts as a broker between the Web server and the Citrix server farm.
3. The Citrix XML Service on the designated server then retrieves from the farm a list of applications that the user can access. These applications comprise the user's *application set*. In MetaFrame XP and MetaFrame 1.8 server farms, the XML Service retrieves the application set from the Independent Management Architecture (IMA) system and Program Neighborhood Service, respectively. In a MetaFrame for UNIX Operating Systems farm, the Citrix XML Service on the designated Citrix server uses information gathered from the ICA Browser and the local NFuse configuration file to determine which applications the user can access.

The Citrix XML Service then forwards the user's application set information to the NFuse Java objects running on the Web server.

4. The Web server uses the NFuse Java objects to generate an HTML page containing links to the applications in the user's application set. Each hyperlink in the HTML page points to a template file stored on the Web server. This file serves as a template from which NFuse can dynamically generate ICA files. *ICA files* are text files containing parameters that configure ICA session properties such as the application to run in the session, the address of the server that will execute the application, and the properties of the window in which to display the application. ICA files are written in .Ini file format and have an .Ica extension.
5. The user initiates the next step by clicking one of the hyperlinks in the HTML page. The Web browser sends a request to the Web server to retrieve an ICA file for the selected application.

The Web server passes this request to the NFuse Java objects, which retrieve the template ICA file. The template file contains substitution tags. The Java objects replace the substitution tags in the template ICA file with information specific to the user and desired application. The Java objects then send the customized ICA file to the Web browser.
6. The Web browser receives the ICA file and passes it to the ICA Client device.
7. The ICA Client receives the ICA file and initiates an ICA session with a Citrix server according to the ICA file's connection information.

System Requirements

The following topics describe the NFuse-specific requirements for each network component in an NFuse system.

Citrix Server Requirements

To work with NFuse Version 1.6, your Citrix servers must meet the following requirements.

Supported MetaFrame Versions

NFuse requires one of the following Citrix platforms:

- MetaFrame XP Application Server for Windows Version 1.0
- MetaFrame Application Server for Windows Version 1.8
- Citrix MetaFrame for UNIX Operating Systems Version 1.1

NFuse operates with these MetaFrame versions on all of their supported platforms. For a list of supported platforms, see your MetaFrame documentation.

Additional Software Requirements

MetaFrame Application Server for Windows Version 1.8 servers must have:

- Citrix MetaFrame 1.8 Service Pack 2 or 3 installed on each server
- Citrix MetaFrame 1.8 Feature Release 1 license installed and activated on each server

Citrix MetaFrame for UNIX Operating Systems Version 1.1 servers must have:

- The Citrix MetaFrame for UNIX Feature Release 1 license installed and activated on each server.
- The Citrix XML Service for UNIX Operating Systems installed on at least one server in the farm. This primary server functions as the contact point between the NFuse Web server and the farm.
- Additional servers running the Citrix XML Service for UNIX Operating Systems are optional for primary server back up.

MetaFrame XP Application Server for Windows Version 1.0 servers have no additional software requirements. Service Pack 1/Feature Release 1 for MetaFrame XP is supported, but not required.

Note DNS address resolution is a new feature in Service Pack 1/Feature Release 1 for MetaFrame XP and Feature Release 1 for MetaFrame for UNIX. To use DNS addresses with NFuse, you must have Service Pack 1 and a Feature Release 1 license installed on all MetaFrame XP servers in a MetaFrame XP farm, or Feature Release 1 installed on all MetaFrame for UNIX servers in a MetaFrame for UNIX farm. See the *MetaFrame Administrator's Guide* for your operating system for more information about DNS address resolution.

General Configuration Requirements

MetaFrame for Windows servers must be members of a server farm. The servers in the farm must have applications published. Additionally, if your Citrix servers are running MetaFrame 1.8 for Windows, you must make sure they have applications published under the server farm management scope. For information about server farm membership and publishing applications in a server farm, see your *MetaFrame Administrator's Guide*.

MetaFrame 1.1 for UNIX Operating Systems servers also must have applications published. In addition, these applications must be configured for use with NFuse. See the *Citrix XML Service for UNIX Operating Systems Administrator's Guide* for information about installing the Citrix XML Service for UNIX and configuring published applications for use with NFuse.

Backward Compatibility

Compatibility issues depend upon the type of server farm in use. Server farms composed of MetaFrame XP 1.0 or MetaFrame 1.8 servers are backward compatible with:

- NFuse Version 1.0
- NFuse Version 1.5
- NFuse Version 1.51

Note When using NFuse 1.0 with MetaFrame XP or MetaFrame 1.8 server farms, the components interoperate by using the down-level NFuse 1.0 XML protocol instead of the updated protocol included in NFuse 1.51 Web Server Extension. Use of the old protocol limits functionality to NFuse 1.0-level features and can create some performance overhead during protocol negotiation.

Server farms composed of MetaFrame for UNIX Operating Systems servers are backward compatible with NFuse Versions 1.5 and 1.51 only.

Web Server Requirements

You can use NFuse on the following Windows/Web server combinations:

- Internet Information Server 4.0 on Windows NT 4.0 Server and Windows NT 4.0 Server, Terminal Server Edition
- Internet Information Server 5.0 on Windows 2000 Server family

You can use NFuse on the following UNIX Web server/operating system/servlet engine/JDK combinations.

Web Server	Operating System	Servlet Engine	JDK
Apache 1.3.20	Redhat 6.2	JServ/GNU JSP *	Sun 1.3.1
		Tomcat 3.2.2	Sun 1.3.1
	Redhat 7.1	JServ/GN UJSP *	Sun 1.3.1
		Tomcat 3.2.2	Sun 1.3.1
	Solaris 7	JServ/GNU JSP *	Sun 1.3.1
		Tomcat 3.2.2	Sun 1.3.1
Solaris 8	JServ/GNU JSP *	Sun 1.3.1	
	Tomcat 3.2.2	Sun 1.3.1	

Web Server	Operating System	Servlet Engine	JDK
iPlanet 4.1	Solaris 7	iPlanet 4.1	Sun 1.3.1
	Solaris 8	iPlanet 4.1	Sun 1.3.1
Tomcat 3.2.2	Redhat 6.2	Tomcat 3.2.2	Sun 1.3.1
	Redhat 7.1	Tomcat 3.2.2	Sun 1.3.1
	Solaris 7	Tomcat 3.2.2	Sun 1.3.1
	Solaris 8	Tomcat 3.2.2	Sun 1.3.1
IBM HTTP 1.3.12.2	Solaris 7	WebSphere 3.5.2	Sun 1.2.2
	Solaris 8	WebSphere 3.5.2	Sun 1.2.2

* JServ 1.2.2 and GNU JSP 1.0.1 and JSDK 2.0

Important Windows NT 4.0 (Server and Terminal Server Edition) ships with Microsoft IIS Version 3.0. Microsoft provides a free upgrade to Microsoft IIS 4.0 in its Windows NT Server 4.0 Option Pack.

Note also that during Microsoft IIS 4.0 installation, the setup program prompts you to install Internet Explorer Version 4 or 5. By default, when you install Internet Explorer Version 4, its setup program installs a Java Virtual Machine on your system. Internet Explorer Version 5 gives you the option to install the JVM instead of placing the JVM on your system by default. Make sure you install the JVM during Internet Explorer Version 5 setup. NFuse requires this JVM for execution of its Web Server Extension software.

When Setup completes, make sure your system has the file Msjava.dll.

The preceding list contains all tested and supported Web server and platform combinations; however, you may be able to use NFuse on other Web servers that support Java servlets and/or JavaServer Pages.

In addition to the NFuse Web Extension, you should have a copy of the ICA Clients on your Web server for Web-based installation of the ICA Clients. See “ICA Client Device Requirements” following for information about supported ICA Client CD-ROM versions. See “Configuring Web-Based ICA Client Installation” on page 43 for information about copying the ICA Clients to the NFuse server.

ICA Client Device Requirements

To operate with NFuse, your ICA Client devices must have a supported ICA Client and a supported Web browser. With the exception of the ICA DOS Client, all ICA Clients that ship on the ICA Client CD are NFuse-compliant. The ICA Client CD is available in your MetaFrame XP Feature Release 1 media, MetaFrame 1.8 Feature Release 1/Service Pack 2 media, Citrix MetaFrame for UNIX Operating Systems Version 1.1 media, or for free download from the Citrix Web site.

Important The ICA Client CD-ROM shipping with the Solaris-only version of MetaFrame for UNIX Operating Systems 1.1 is not compatible with NFuse. Users of these systems must download the latest ICA Clients from the Citrix Web site at <http://www.citrix.com/download> before beginning NFuse deployment.

In addition to the ICA Clients on the ICA Client CD-ROM, some previously shipped ICA Clients are NFuse-compliant as well. The following table lists minimum ICA Client version levels for supported browsers.

ICA Client	Version	Supported browsers
Win32	6.1.963 and above	Internet Explorer 4.01 and above Netscape Communicator 4.77 and above Netscape Navigator 6.01 and above
Win16	6.1.961 and above	Internet Explorer 4.01 and above Netscape Navigator 4.08 and above
Java	6.0.1146 and above	Internet Explorer 4.01 and above Netscape Communicator 4.77 and above Netscape Navigator 6.01 and above
Macintosh	6.0.66 and above	Internet Explorer 4.01 and above Netscape Communicator 4.77 and above Netscape Navigator 6.01 and above
UNIX for Compaq/Tru64	3.0.42 and above	Netscape Communicator 4.77 and above Netscape Navigator 6.01 and above
UNIX for HP/UX	3.0.42 and above	Netscape Communicator 4.77 and above Netscape Navigator 6.01 and above

ICA Client	Version	Supported browsers
UNIX for IBM AIX	3.0.42 and above	Netscape Communicator 4.77 and above Netscape Navigator 6.01 and above
UNIX for Linux/ ARM	3.0.86 and above	Netscape Communicator 4.77 and above Netscape Navigator 6.01 and above
UNIX for SCO	3.0.36 and above	Netscape Communicator 4.77 and above Netscape Navigator 6.01 and above
UNIX for SGI	3.0.42 and above	Netscape Communicator 4.77 and above Netscape Navigator 6.01 and above
UNIX for Solaris/ Sparc	6.0.915 and above	Netscape Communicator 4.77 and above Netscape Navigator 6.01 and above
UNIX for Solaris/ x86	3.0.35 and above	Netscape Communicator 4.77 and above Netscape Navigator 6.01 and above
UNIX for SunOS	3.0.35 and above	Netscape Communicator 4.77 and above Netscape Navigator 6.01 and above

The features and capabilities of each ICA Client differ. For information about supported ICA Client features, see the *Citrix ICA Client Administrator's Guide* for the ICA Client in question.

Overview of this Manual

This manual contains the following chapters:

- Chapter 3: “Configuring Your Web Server” on page 23 - Describes how to prepare your Web server to participate in an NFuse system. Topics covered include installing the Citrix Web Server Extension on your Web server and configuring NFuse.
- Chapter 4: “Configuring ICA Client Devices” on page 43 - Describes steps required to prepare your ICA Client devices. Includes information about using Web-based ICA Client installation to deploy and install ICA Clients. Explains additional configuration required by some ICA Clients to work with NFuse.
- Chapter 5: “Configuring NFuse Security” on page 51 - Describes security considerations and lists measures you can take to secure your NFuse system.
- Chapter 6: “ICA Program Neighborhood Agent Configuration” on page 59 - Describes how to use the Config.xml file to customize the Program Neighborhood Agent.

What to Do Next

NFuse deployment begins with configuration of your Web server. For information, see Chapter 3, “Configuring Your Web Server” on page 23.

Configuring Your Web Server



This chapter explains how to install and configure the NFuse Web server extension on your Web server. When you install NFuse, it also installs Web pages that users can use to access their application sets. When NFuse is installed and configured, you just inform your users of the URL for the NFuse Login page.

Feature Release 1 includes NFuse version 1.6. If NFuse was installed during MetaFrame XP installation, installing Feature Release 1 / Service Pack 1 will upgrade NFuse to version 1.6. If you have NFuse installed on a separate Web server, the decision to upgrade to NFuse 1.6 is up to you. Whether you upgrade to version 1.6 or not, NFuse continues to work with MetaFrame XP with Feature Release 1 and Service Pack 1 installed.

Tasks to Complete

In this chapter Web server administrators will:

- Install the Citrix Web Server Extension on a Web server and configure the Web server if necessary
- Configure the Web Server Extension properties

Web Server Extension Installation

NFuse includes separate setup programs for installing the Web Server Extension on various Web servers. The topics that follow explain how to use these setup programs to install the Web Server Extension on:

- Microsoft Internet Information Server (IIS)
- iPlanet Web Server and Apache Server for UNIX platforms

If you are upgrading a previous installation of the Web Server Extension, see the following section before proceeding.

Upgrading Existing NFuse Installations

This release of NFuse supports the following upgrade paths:

Upgrading a Web Server Extension installed with MetaFrame XP during Feature Release 1/Service Pack 1 Installation. If you installed the NFuse Web Server Extension during MetaFrame XP installation, the example Web site is located in a MetaFrame subdirectory of the webroot directory. Feature Release 1/Service Pack 1 Setup backs up these files to %SystemRoot%\mfxp10sp1 and installs the NFuse version 1.6 Web pages in their place. Settings in the NFuse 1.51 NFuse.properties file are migrated to the NFuse 1.6 NFuse.conf file. If you uninstall Feature Release 1/Service Pack 1, your previous installation of NFuse is restored.

Upgrading a stand-alone Web Server Extension using the NFuse 1.6 CD. If you installed a previous version of the NFuse Web Server Extension from the NFuse CD, it placed the example Web sites into a \NFuse, \Citrix\NFuse15, or \Citrix\NFuse151 subdirectory of the webroot directory. When you install the NFuse 1.6 Web Server Extension from the NFuse 1.6 CD, it installs the NFuse 1.6 Web pages in a \Citrix\NFuse16 subdirectory of the webroot directory. Setup prompts you to specify a directory to backup the old NFuse Java object and properties files. You must manually migrate any customizations made to these files into your new installation. If you uninstall NFuse 1.6, you must then move the old NFuse Java object and properties files from the backup directory to their previous locations to restore NFuse 1.51 functionality.

Installing NFuse During MetaFrame XP Installation

MetaFrame XP Setup offers administrators the option of installing NFuse during MetaFrame installation. This option installs the Web Server Extension on the server and places the NFuse Web pages in the Web document root directory. The Web site is a fully-functional NFuse site and can be used as-is with no additional configuration. If you choose to change your default Web page, the default Web page for your MetaFrame server is the NFuse Login page.

If you want to use NFuse 1.6, you must install MetaFrame XP Feature Release 1 / Service Pack 1 after MetaFrame XP installation is completed.

Installing the Web Server Extension on Microsoft IIS

During Web Server Extension installation, you must identify one or more MetaFrame servers in your farm that will act as contact points between the server farm and your Web server. The names you specify can be Windows NT server names, IP addresses, or fully-qualified DNS names. If your server farm is composed of MetaFrame for Windows servers, you can specify the name of any server in the farm. If your server farm is composed of MetaFrame for UNIX Operating Systems servers, you must specify the name of servers running the Citrix XML Service for UNIX Operating Systems.

In addition, you must specify the TCP/IP port on which the specified servers are running the Citrix XML Service. If you do not know this port number, you can determine it by checking a MetaFrame server's port information.

► **To view the XML Service port assignment**

- On MetaFrame XP servers, open the Citrix Management Console. In the left pane, right-click the server and select **Properties**. In the **Properties** dialog box, select the **MetaFrame Settings** tab to view the port assignment.

Note that if during MetaFrame XP installation the administrator chose the option to share Internet Information Server's TCP/IP port with NFuse, the Citrix Management Console displays **Sharing with IIS** as the port in use. In this case, to determine the XML Service port you must locate the port used by Internet Information Server's WWW Service. By default the WWW Service uses port 80.

- On MetaFrame 1.8 servers, the port number is specified in the following registry key:

```
HKLM\SYSTEM\CurrentControlSet\Services\CtxHttp\TcpPort
```

- On MetaFrame for UNIX Operating Systems servers, type **ctxnfusesrv -l** at a command prompt to view port information.

Note If necessary, you can change the port used on the MetaFrame server. For MetaFrame 1.8 servers, see the *Feature Release 1 and Service Pack 2 Installation Guide for Citrix MetaFrame for Windows Version 1.8*. For MetaFrame XP servers, see the installation chapter of the *MetaFrame XP Administrator's Guide*. For MetaFrame for UNIX servers, see the *Citrix XML Service for UNIX Operating Systems Administrator's Guide*.

Towards the end of Web Server Extension installation, the setup program prompts you to supply an ICA Client CD or CD image. Setup copies the contents of the CD's ICAWEB directory to a directory called /Citrix/ICAWEB that it creates off the Web server's Web publishing root. All Web sites created by the installation process assume that the Web server contains the ICA Client files in this directory structure. If you do not want to copy the ICA Clients to the Web server during Web Server Extension installation, you can copy them to the server later. Make sure you create the required directory structure; for example, in an English installation: `<webroot>/Citrix/ICAWEB/en/<icaclientversion>`.

Important During installation or uninstallation of Web Server Extension on Microsoft IIS, the setup program stops and then restarts your Web server and all of its associated services. This restart causes a disruption of service to connected users for the duration of the installation.

► **To install the Web Server Extension on Microsoft IIS**

1. Make sure you are logged on as a user with administrator privileges.
2. If you are installing the Web Server Extension from an NFuse CD-ROM included in your MetaFrame XP Feature Release 1 media, insert the CD-ROM in your Web server's CD-ROM drive. Locate the file named NFuseWebExtSetup-IIS.exe. Double-click the file.

If you downloaded the Web Server Extension from a download site, copy the file NFuseWebExtSetup-IIS.exe to your Web server. Double-click the file.

3. The Installation wizard guides you through installation.
See Chapter 4, "Configuring ICA Client Devices" on page 43 for information about securing your Web server.

Plugging the Citrix XML Service into IIS

Internet Information Server can be used to perform some tasks associated with the Citrix XML Service. This procedure is not a required step in Web server configuration and is intended for those administrators who want to integrate the functionality of the Citrix XML Service with a Web server's HTTP service. Plugging the XML Service into IIS lets you use a single TCP/IP port for both Web server and NFuse traffic and eliminates the need for opening additional ports for NFuse in network firewalls.

Note This procedure is a manual version of the automatic Internet Information Server extension configuration performed by MetaFrame XP Setup. If you are using a MetaFrame XP server as your Web server and did not choose to share the XMP port with IIS during MetaFrame XP installation, use this procedure to manually plug the XML Service into your Web server.

The Citrix XML Service contains an ISAPI extension that you can plug into Internet Information Server. The XML Service contains the following components:

- **Ctxxmlss.exe.** This network component is a relay for NFuse data requests. The NFuse Java objects send application set requests to Ctxxmlss.exe, which passes the requests to Wpnbr.dll (described below) for processing. Ctxxmlss.exe then forwards the information returned by Wpnbr.dll to the Java objects that requested the data.
- **Wpnbr.dll and Clm.dll.** These .Dll files communicate with the Program Neighborhood Service or Independent Management Architecture (IMA) systems in the farm to determine application set information for a user or user group.

Plugging the Citrix XML Service into IIS involves using IIS as the relay for NFuse data requests. In this configuration, IIS replaces Ctxxmlss.exe as the network listener and Wpnbr.dll and Clm.dll execute as an ISAPI extensions to IIS.

The following procedure describes how to plug the Citrix XML Service into your IIS Web server.

► **To plug the Citrix XML Service into IIS**

1. Locate the following files on a MetaFrame server that has Service Pack 2 or MetaFrame XP installed: Wpnbr.dll, Ctxxmlss.txt, and Clm.dll. The default installation location is %SystemRoot%\System32\.
2. Copy these files into the IIS scripts directory on your Web server. For example, the default scripts directory on IIS Version 5.0 is <RootDrive>:\inetpub\scripts\.
3. Use Internet Service Manager to give these two files Read and Write access.
4. Edit the **SessionField.NFuse_CitrixServer** parameter in NFuse.conf file to specify the address of the NFuse Web server and the and **SessionField.NFuse_CitrixServerPort** parameter to specify the IIS port (80 by default).
5. Stop and restart the Web server service.

Installing the Web Server Extension on iPlanet Web Server and Apache Server

The Setup program for installing the Web Server Extension on iPlanet Web Server and Apache Server prompts you for locations in which to place various NFuse files. The following table lists these files by type. Use this table as a reference when installing the Web Server Extension and configuring your Web server.

File Type	Description	Directory
NFuse Java objects: nfuse.jar ctxxml4j.jar jsafeObj.jar sslplus3.1.7.jar	Java objects including the base NFuse Class files, IBM XML parser, and SSL/SOCKS provider Classes and cryptographic libraries.	You can copy these files to any directory.
Properties files: NFuse.conf NFuse.properties NFuse.dtd NFuse.txt NFuseClientDetectStrings.properties NFuseErrorsResource.properties	Text files containing NFuse configuration parameters, XML definitions, display strings, error message strings, and Web-based ICA Client installation strings.	The setup program copies these files to the directory you specify for the NFuse Java objects.
Web pages	NFuse Web pages	Place these files in any directory from which your Web server can serve Web pages. The setup program defaults to the directory <webroot>/Citrix/NFuse16.

File Type	Description	Directory
Icon files	The setup program creates an icon cache directory that the NFuse Java objects use to store application icons (.Gif files).	Place this directory in any location from which your Web server can serve Web pages. The setup program defaults to the <webroot>/NFuseicons directory. If you change the path from the default, you must update the SessionField.NFuse_IconCache parameter in the NFuse.conf file.
ICA Clients	Citrix ICA Client installation files used by NFuse Web sites to install ICA Clients on client devices.	The setup program prompts the administrator to supply an ICA Client CD or CD image and then copies the contents of the CD's ICAWEB directory to a /Citrix/ICAWEB directory off the Web server's Web publishing root. The NFuse Web pages assume the ICA Client files are stored in this directory structure. If the ICA Client CD is not available, you can copy the contents of the CD's ICAWEB directory to your Web server after setup completes.

During Web Server Extension installation, you must identify a MetaFrame server in your farm that will act as a contact point between the server farm and your Web server. The name you specify can be a Windows NT server name, IP address, or fully-qualified DNS name. If your server farm is composed of MetaFrame for Windows servers, you can specify the name of any server in the farm. If your server farm is composed of MetaFrame for UNIX Operating Systems servers, you must specify the name of a server running the Citrix XML Service for UNIX Operating Systems.

In addition, you must specify the TCP/IP port on which the specified server is running the Citrix XML Service. If you do not know this port number, you can determine it by checking the MetaFrame server's port information.

► **To view the XML Service port assignment**

- On MetaFrame XP servers, open the Citrix Management Console. In the left pane, right-click the server and select **Properties**. In the **Properties** dialog box, select the **MetaFrame Settings** tab to view the port assignment.

Note that if the administrator chose the option to share Internet Information Server's TCP/IP port with NFuse during MetaFrame XP installation, the Citrix Management Console displays **Sharing with IIS** as the port in use. To determine the XML Service port in this case, you must locate the port used by Internet Information Server's WWW Service. By default the WWW Service uses port 80.

- On MetaFrame 1.8 servers, the port number is specified in the following registry key:
HKLM\SYSTEM\CurrentControlSet\Services\CtxHttp\TcpPort
- On MetaFrame for UNIX Operating Systems servers, type **ctxnfusesrv -l** at a command prompt to view port information.

Note If necessary, you can change the port in use on the MetaFrame server. For MetaFrame 1.8 servers, see the *Feature Release 1 and Service Pack 2 Installation Guide for Citrix MetaFrame for Windows Version 1.8*. For MetaFrame XP servers, see the installation chapter of the *MetaFrame XP Administrator's Guide*. For MetaFrame for UNIX servers, see the *Citrix XML Service for UNIX Operating Systems Administrator's Guide*.

Web Server Extension installation prompts you to enter a virtual URL for servlets. The value you enter must match the virtual URL you specify later when configuring your Web server to run NFuse. See “Configuring iPlanet Web Server” on page 31 and “Configuring Apache Server” on page 32 for more information about NFuse’s use of virtual URLs for servlets.

► **To install the Web Server Extension on iPlanet Web Server and Apache Server**

1. Log on as root at the server on which you want to install the Web Server Extension.
2. Copy the Web Server Extension file for UNIX (NFuseWebExtSetup-UNIX.tar.gz) from your NFuse CD-ROM or the Citrix download site to an install directory on your Web server.
3. Unzip the NFuseWebExtSetup-UNIX.tar.gz file. Unzipping the file produces NFuseWebExtSetup-UNIX.tar, an archive containing the setup files for NFuse.
4. To extract the archived files from NFuseWebExtSetup-UNIX.tar into the install directory, type **tar xvf NFuseWebExtSetup-UNIX.tar** and press ENTER.
5. Stop your Web server.
6. Type **./setupNFuse** to begin the installation.
7. Follow the instructions on the screen to install the NFuse files in the appropriate directories. See the table at the beginning of this section for a detailed description of NFuse’s files and directories in which you must place them.

8. Toward the end of Web Server Extension installation, the setup program prompts you to supply an ICA Client CD-ROM or CD-ROM image. Setup copies the contents of the CD-ROM's ICAWEB directory to a directory called / /Citrix/ICAWEB that it creates off the Web server's Web publishing root. All NFuse Web pages assume that the Web server contains the ICA Client files in this directory structure. If you do not want to copy the ICA Clients to the Web server during Web Server Extension installation, you can copy them to the server later. Make sure you create the required directory structure; for example, in an English installation: `<webroot>/Citrix/ICAWEB/en/<icaclientversion>`.
9. Restart your Web server.

After you complete the installation, you must configure your Web server. For information about configuring iPlanet Web Server, see "Configuring iPlanet Web Server" below. For information about configuring Apache Server, see "Configuring Apache Server" on page 32.

See Chapter 8, "Configuring NFuse Security" on page 51 for information about securing your Web server.

Configuring iPlanet Web Server

The following procedures explain how to configure iPlanet Web Server for NFuse.

► To configure iPlanet Web Server 4.1 for NFuse

1. Log on to Adminserv. Click the **Global Settings** tab. In the left pane, click **Configure JRE/JDK Paths** and select **JDK**. In the **JDK Path** field, make sure that the path to the JDK is correct.
2. Click the **Servers** tab. Make sure your server is selected and click **Manage**.
3. Click the **Servlets** tab. Enable the Servlet Engine and JSP if they are not enabled already.
4. In the left pane, click **Configure JVM Attributes**. In the **Classpath** field, add the following:
 - The full path to the file `nfuse.jar`.
 - The full path to the file `ctxml4j.jar`.
 - The full path to the file `jsafeObf.jar`.
 - The full path to the file `sslplus3.1.7.jar`.
 - The full path to the directory containing the `NFuse.properties` and `NFuseErrorsResource.properties` files.
5. Restart the Web server.

Configuring Apache Server

The following instructions explain how to set up NFuse on an Apache Server running JServ and GNUJSP. These instructions assume that you have already installed Apache, JServ, and GNUJSP and have verified that basic “Hello World” examples for both Java Servlets and JavaServer Pages are working. If you want to use Java servlets only and do not intend to deploy any NFuse JavaServer Pages-based sites, you can ignore the instructions regarding GNUJSP.

Note The following instructions use a single servlet zone for NFuse Web sites. NFuse may not work properly if invoked from more than one servlet zone. It is important that all your NFuse pages, whether JavaServer Page or HTML for Servlets-based, use the same zone.

► To configure Apache Server

1. Open the configuration file `httpd.conf` located in your Apache installation's configuration directory; for example, `/usr/local/apache/conf/httpd.conf`.
2. If you installed and tested JServ, the following lines appear somewhere in `httpd.conf`:

```
<IfModule mod_jserv.c>
    .
    .
    .
</IfModule>
```

These lines configure Apache to send certain HTTP requests to the JServ servlet engine. Add or modify the following lines:

```
<IfModule mod_jserv.c>
    .
    .
    .
    ApJServMount /servleturl /NFuseJservZone
    ApJServMount /jspurl /NFuseJservZone
    ApJServAction .jsp /jspurl/gnujsp
    .
    .
    .
</IfModule>
```

where:

/servletsurl is a virtual URL for which Apache will redirect HTTP requests to the JServ servlet engine when serving NFuse HTML for Servlets pages. This virtual URL must be the same virtual URL as entered during NFuse setup.

/NfuseJServZone is the name of the JServ zone for NFuse. For information about JServ zones, see the JServ documentation. The name for this zone appears in the JServ configuration file described later.

/jspurl is the virtual URL for which Apache will redirect HTTP requests to the JServ servlet engine when serving NFuse .Jsp pages. Apache uses this virtual URL internally; the name you specify can be any name that doesn't conflict with other URLs.

/gnujsp is the name of the GNUJSP servlet alias as it appears in the GNUJSP zone configuration file described later. For default GNUJSP installations, this alias is “/gnujsp”.

Note The names specified above are placeholders. You do not have to specify the same names for your deployment.

3. Now you must modify the JServ configuration files. Open the master JServ configuration file. This file is usually named `jserv.properties` and is often located in the `conf` subdirectory of the JServ installation; for example, `/usr/local/jserv/conf/jserv.properties`.
4. If it is not already there, add your NFuse JServ zone to the list of zones. The file should contain a line such as:
`zones=otherzone1, otherzone2`
Modify such a line so that it reads:
`zones=otherzone1, otherzone2, NfuseJServZone`
where *NfuseJServZone* is the name of the NFuse JServ zone specified in Step 2 above.
5. Now you must specify the NFuse JServ zone configuration file in the master JServ configuration file. Somewhere in the master JServ configuration file, add the following line:
`NfuseJServZone.properties=path-to-JServ-conf-directory/
NfuseJServZone.properties`
where *NfuseJServZone* is the name of the NFuse JServ zone specified in Step 2 above and *path-to-JServ-conf-directory* is the directory that contains `jserv.properties`

6. Now create the NFuse JServ zone configuration file. Create this file in the directory specified in Step 5 as *path-to-Jserv-conf-directory/NFuseJServZone.properties*.

If you are *not* using GNUJSP, you can create this file by copying the default JServ zone configuration file called `zone.properties` from your JServ distribution.

If you are using GNUJSP, follow the installation instructions in your GNUJSP distribution to create your NFuse JServ configuration file. Make sure the name of the alias for the GNUJSP servlet is the same as specified in Step 2 above.

7. Add the NFuse jar files (`nfuse.jar`, `ctxxml4j.jar`, `jsafeObf.jar`, and `sslplus3.1.7.jar`) to the list of repositories in your NFuse JServ zone configuration file.

For example, if you installed the NFuse objects in `/usr/local/jserv/NFuse` when you installed NFuse, you add or modify the following lines in your NFuse JServ zone configuration file:

```
repositories=/usr/local/jserv/NFuse
repositories=/usr/local/jserv/NFuse/nfuse.jar
repositories=/usr/local/jserv/NFuse/ctxxml4j.jar
repositories=/usr/local/jserv/NFuse/jsafeObf.jar
repositories=/usr/local/jserv/NFuse/sslplus3.1.7.jar
```

8. Stop and restart both Apache and JServ.

Configuring Web Server Extension Properties

The Web Server Extension includes a configuration file that lets you change several of NFuse's properties. The file `NFuse.properties`, located in the same directory as the NFuse Java objects (`nfuse.jar`, `ctxxml4j.jar`, `jsafeObf.jar`, and `sslplus3.1.7.jar`), specifies the path and encoding method for the file `NFuse.conf`. The configuration settings are contained in the `NFuse.conf` file. By default, both files are stored in the same directory as the NFuse Java objects.

The `NFuse.properties` file contains the following parameters:

- **ConfigurationFileEncoding.** Specifies the encoding used for `NFuse.conf`. Use basic Latin on English, French, German, and Spanish servers. Use Shift-JIS Japanese on Japanese server. Specify "8859_1" for basic Latin or "SJIS" for Shift-JIS Japanese on Windows Web servers. Specify "ISO8859_1" for basic Latin or "SJIS" for Shift-JIS Japanese on UNIX Web servers.

-
- **ConfigurationFilePath.** Specifies the path and file name of the NFuse.conf file. If you move NFuse.conf, you must modify this value. The default value is *D:\WINNT\Java\TrustLib\NFuse.conf*, where *D:\WINNT* is the drive and path where Windows is installed.

Important The settings in NFuse.conf are global: all Web pages generated by the Web Server Extension draw from the file's values. Changes made to NFuse.conf affect all Web pages served by the Web Server Extension.

If necessary, you can override values in NFuse.conf on a per-page basis in your Web server scripts; for example, if you want to use multiple MetaFrame servers acting as communication links to the Web server. For more information about Web server scripts, see the NFuse SDK.

Important For changes made to NFuse.properties or NFuse.conf to take effect, you must stop and restart your Web server. For Microsoft Internet Information Server, use Control Panel to stop and restart IIS Admin Service and all of its dependent services. Restarting IIS Admin Service does not restart the dependent services; you must restart the dependent services manually.

NFuse.conf can contain the following parameters. If a parameter is not specified in the file, the default value is used.

Parameter	Default Value	Description
SessionField.NFuse_ContentType	text/html	Sets the MIME type of pages produced by the NFuse Java objects to the specified value. The default value is text/html.
SessionFieldLocations	PNAgent, Script, Template, Url, Post, Cookie, Properties	<p>Specifies the valid locations for setting session fields. If a field is set in multiple locations, the location earlier in the list takes precedence.</p> <p>PNAgent - Session field set in Program Neighborhood Agent script files or template.ica file.</p> <p>Script - Session field set in a Web page by a TemplateParser's setSessionField() method.</p> <p>Template - Session field set using the [NFuse_SetSessionField] session field in a template file.</p> <p>URL - Session field set using the Get method in an HTML form.</p> <p>Post - Session field set using the Post method in an HTML form.</p> <p>Cookie - Session field set in a cookie.</p> <p>Properties - Session field set in NFuse.conf.</p>
Timeout	60	Specifies a communication timeout value, in seconds. When the Java objects establish communication with a MetaFrame server, each subsequent Java object query of the MetaFrame server is subject to the specified timeout value. If the server does not respond to a Java object request within the allotted time, the operation times out.
Version	1.6	Do not edit this parameter.
SessionField.NFuse_CitrixServer	N/A	<p>Specifies the name of one or more MetaFrame servers in the farm. These servers are the communication link between the server farm and the Web server. The default value is the server name entered during Web Server Extension installation. The server name can be a Windows NT server name, IP address, or fully-qualified DNS name.</p> <p>If an error occurs while communicating with a server, the next server on the list is tried. If communication succeeds, all further communication is with that server until there is another error. The NFuse Web server does not revert to failed MetaFrame servers. The only way to make the NFuse Web server use failed MetaFrame servers is to reset the Web server.</p>
SessionField.NFuse_CitrixServerPort	80	<p>Specifies the TCP/IP port used by the Citrix XML Service on the MetaFrame servers specified in NFuse_CitrixServer. The default value is the port number entered during Web Server Extension installation. This port number must match the port number used by the Citrix XML Service.</p> <p>If you specify multiple MetaFrame servers in the SessionField.NFuse_CitrixServer parameter, they must all have the Citrix XML Service configured on the same port.</p>

Parameter	Default Value	Description
AlternateAddress	off	Specifies whether to use alternate address translation of the MetaFrame server address specified in the .lca files that are sent to client devices to launch ICA sessions. If the value is "on", the external address of MetaFrame servers is included in .lca files generated by NFuse. If the value is "off", no alternate address translation is performed. The external address of MetaFrame servers is configured with the ALTADDR command. For more information, see the description for the ALTADDR command in Appendix A of the <i>MetaFrame XP Administrator's Guide</i> .
SessionField.NFuse_RelayServer	none	Specifies the name of the MetaFrame server on which the SSL Relay is running. The server name can be a Windows NT server name, IP address, or fully-qualified DNS name. Make sure the naming format you specify is consistent with the name specified in your SSL Relay server's certificate; for example, specify a DNS name if the certificate contains a DNS name. By default, this parameter is not included in the NFuse.conf file.
SessionField.NFuse_RelayServerPort	none	Specifies the TCP port of the SSL Relay. By default, this parameter is not included in the NFuse.conf file.
SessionField.NFuse_IconCache	/NFuselcons/	Specifies the directory used to store NFuse-generated application icon files (.Gif). The default value is /NFuselcons/ on Internet Information Server and /NFuseicons/ on UNIX Web servers. On Internet Information Server, the Internet guest account must have Read, Write, List, and Delete access to this directory. On UNIX Web servers, the files must be World readable and the directory must be World readable and executable.
SessionField.NFuse_TemplatesDir	d:\inetpub\wwwroot\Citrix\MetaFrame	Specifies the directory where a TemplateParser object looks when a template file is specified with the NFuse_Template session field.
URLMapping./	d:\inetpub\wwwroot	Specifies the path to your Web server's Web publishing root directory; for example, in many Microsoft Internet Information Server systems, the URLMapping./ entry specifies C:\inetpub\WWWRoot.
HttpInputEncoding	8859_1	Specifies the encoding ¹ used for incoming HTTP such as form data.
HttpOutputEncoding	8859_1	Specifies the encoding ¹ used for outgoing HTTP such as HTML pages that display application sets.
TemplateFileEncoding	8859_1	Specifies the encoding ¹ used for Citrix HTML template files.
CacheExpireTime	3600	Specifies the default expiration timeout value in seconds for the AppDataList objects stored in the AppListCache object. Used for caching of application set information about the Web server. See the descriptions of example NFuse Web pages in <i>Configuring NFuse 1.6</i> for more information on application caching.
SessionField.NFuse_TicketTimeToLive	200	Specifies the amount of time in seconds for which an authentication ticket is valid. A ticket that is older than the specified duration cannot successfully authenticate a user to the MetaFrame server farm.

Parameter	Default Value	Description
SessionField.NFuse_Transport	HTTP	Specifies the protocol used to transport NFuse data between the Web server and Citrix server specified in NFuse_CitrixServer . Values include "HTTP" and "SSL." Use HTTP to send the NFuse data over a standard HTTP connection to the server and port specified in NFuse_CitrixServer and NFuse_CitrixServerPort . Use SSL to send data over a secure connection that uses a Citrix server running the Citrix SSL Relay to perform host authentication and data encryption. This protocol sends the data to the server and port specified in NFuse_CitrixServer and NFuse_CitrixServerPort through a Citrix SSL Relay server specified in NFuse_RelayServer and NFuse_RelayServerPort .
SslKeystore	D:\WINNT\keystore\cacerts	Specifies the directory containing the certificate authority root certificates. NFuse uses root certificates when authenticating a Citrix SSL Relay server.
DTDDirectory	D:\WINNT\System32	Specifies the directory containing the NFuse DTD file. The default is the Java Virtual Machine's working directory.
AllowCustomizeWinSize	on	Specifies whether users can adjust the window size for ICA sessions from the NFuse Settings page. See AllowCustomize Settings for more information.
AllowCustomizeWinColor	off	Specifies whether users can adjust the color depth for ICA sessions from the NFuse Settings page. See AllowCustomize Settings for more information.
AllowCustomizeAudio	off	Specifies whether users can adjust the audio quality for ICA sessions from the NFuse Settings page. See AllowCustomize Settings for more information.
AllowCustomizeEncryption	off	Specifies whether users can adjust the encryption level for ICA sessions from the NFuse Settings page. See AllowCustomize Settings for more information.
AllowCustomizeSettings	on	<p>If the value is set to "on" the user has access to the NFuse Settings page. This page has options for "Remember Folder Location," "Show Current Folder Location," "Application Detail Display," and other settings that are controlled by parameters in the NFuse.conf file.</p> <p>For each of the AllowCustomize* parameters, if the value is set to "on," users can edit the setting on the NFuse Settings page. If the value is "off," the setting is not displayed in the NFuse Settings page and the settings specified for the published application in the Citrix Management Console are used.</p> <p>User-specific settings are stored as cookies on the client device. Depending on the operating system and Web browser used, these cookies may be specific to each user or all users will have the same settings. Customized settings made by users logged in as a guest (using an AnonXXX account) are not saved to the client device.</p>

Parameter	Default Value	Description
AllowGuestLogin	off	<p>If the value is set to “on,” a Guest User option appears on the NFuse Login page. Guest users can only run published applications that allow anonymous user connections. NFuse Guest users actually use the AnonXXX accounts created by MetaFrame.</p> <p>If the value is set to “only,” the login/logout capabilities of the Web site are disabled and only anonymous applications are displayed. If the value is set to “off,” Guest logins are not permitted.</p>
AddressResolution Type	ipv4-port	<p>Specifies what type of address to use for the NFuse_AppServerAddress tag in Template.ica. Possible values are Ipv4, Ipv4-port, dns, and dns-port. Citrix recommends using either ipv4-port or dns-port address resolution.</p> <p>Note - The dns and dns-port values require DNS address resolution, which is only available in MetaFrame XP with Feature Release 1. See the <i>MetaFrame Administrator's Guide for MetaFrame XP for Windows, Feature Release 1</i> for more information about DNS address resolution.</p>
ForceClient Installation	off	<p>If the value is set to “on,” the client installation caption and download links are always shown. If the value is set to “off,” the client installation caption and download links are displayed only if no ICA Client is detected on the client computer. Client detection is currently supported only for 16-bit and 32-bit Windows platforms. For other platforms, the installation and caption download links are always displayed, regardless of whether the ICA Client is already installed.</p> <p>See the description for Win32Client for information about customizing the installation captions and download links.</p>
OtherClient	default	<p>Specifies captions and links for unrecognized client platforms. The default value is to display a link to the ICA Java Client. See the description for Win32Client for information about specifying custom links.</p>
OverrideClientInstall Caption	none	<p>Specifies a custom message to be displayed along with the download links for the ICA Clients. By default, this parameter is commented out by a pound symbol or hash mark (#) at the beginning of the line and the default messages are used. The default message is specific to the identified client platform, and is similar to the following:</p> <p style="padding-left: 40px;">You do not have the Citrix ICA Client (ActiveX) for 32-bit Windows installed on your system. You must install the ICA Client to launch the applications.</p> <p style="padding-left: 40px;">Select the icon below to install the ICA Client.</p>
Win32Client	default	<p>If the value is set to “default,” the default ICA Client links for this platform are displayed in the NFuse Message Center. The links are to the ICA Win32 Web client located at wwwroot\Citrix\ICAWEB.</p> <p>Captions and links can be customized using the format “caption1&url,caption2&url2,....caption&urlN” where caption is the display text and url is the URL for the ICA Client. The caption is shown in the NFuse Message Center portion of the NFuse Login page as a hyperlink to the specified URL.</p>

Parameter	Default Value	Description
Win16Client	default	Specifies captions and links for 16-bit Windows Client platforms. See the description for Win32Client for information about specifying custom links.
SolarisUnixClient	default	Specifies captions and links for Solaris Client platforms. See the description for Win32Client for information about specifying custom links.
JavaClient	default	Specifies captions and links for Java Client platforms. See the description for Win32Client for information about specifying custom links.
MacClient	default	Specifies captions and links for Macintosh Client platforms. See the description for Win32Client for information about specifying custom links.
SgiUnixClient	default	Specifies captions and links for SGI UNIX Client platforms. See the description for Win32Client for information about specifying custom links.
HpUxUnixClient	default	Specifies captions and links for HP-UX Client platforms. See the description for Win32Client for information about specifying custom links.
IbmAixClient	default	Specifies captions and links for IBM-AIX Client platforms. See the description for Win32Client for information about specifying custom links.
ScoUnixClient	default	Specifies captions and links for SCO UNIX Client platforms. See the description for Win32Client for information about specifying custom links.
Tru64Client	default	Specifies captions and links for Tru64 UNIX Client platforms. See the description for Win32Client for information about specifying custom links.
LinuxClient	default	Specifies captions and links for Linux Client platforms. See the description for Win32Client for information about specifying custom links.
LoginType	default	<p>If “default” is specified, use Microsoft domain-based authentication. If “nds” is specified, use Novell NDS authentication.</p> <p>Note - To use NDS authentication, you must specify an NDS tree using the NDSTreeName parameter.</p> <p>Note - This setting does not affect the authentication method used for ICA Program Neighborhood Agent Clients. You must edit the Config.xml file to change the authentication method for Program Neighborhood Agent Clients. See Chapter 6, “ICA Program Neighborhood Agent Configuration” on page 59 for more informaton on editing the Config.xml file.</p>
ForceLoginDomain	none	<p>When using Microsoft domain-based authentication, you can force all users to log in to a specific domain by specifying the domain as the value. By default, this parameter is commented out by a pound symbol or hash mark (#) at the beginning of the line. When commented out, users must type the name of the domain in the NFuse Login page. When a value is specified, the domain is not displayed to users on the NFuse Login page.</p> <p>When using NDS authentication, you can force users to type their user principal name (UPN) in the user name box by removing the pound symbol (#) at the beginning of the line and defining this parameter with a blank value.</p>

Parameter	Default Value	Description
NDSTreeName	none	When using NDS authentication, you must specify the NDS tree to use for authenticating users. By default, this parameter is commented out by a pound symbol or has mark (#) at the beginning of the line.
SearchContextList	none	If you set the value to a comma-delimited list of context names, the context lookup for users is performed only within this list of contexts. If this parameter is not specified, a context lookup is performed for users on all contexts in the tree. By default, this parameter is commented out by a pound symbol or has mark (#) at the beginning of the line.
StaticStringTextFile	D:\WINNT\java\trustlib\nfuse.txt	Specifies the path to the static string file. This file contains all of the text used by the NFuse Web server extension. Note - Editing the nfuse.txt file is not supported.
StaticStringTextFile Encoding	8859_1	Specifies the encoding ¹ used for the static string file.

¹ Encoding options: Specifies the encoding used for NFuse.conf. Use basic Latin on English, French, German, and Spanish servers. Use Shift-JIS Japanese on Japanese server. Specify “8859_1” for basic Latin or “SJIS” for Shift-JIS Japanese on Windows Web servers. Specify “ISO8859_1” for basic Latin or “SJIS” for Shift-JIS Japanese on UNIX Web servers.

Making NFuse Available to Users

Now that NFuse is installed and configured, you need to inform your users of the URL for the NFuse Login page. For NFuse servers installed as part of MetaFrame XP, if you choose to change your default Web page, the default Web page for your MetaFrame server (<http://servername>) is the NFuse Login page. Otherwise, the URL is <http://servername/Citrix/MetaFrame>.

For NFuse servers installed on a separate Internet Information Server or Apache Server system, the URL is <http://servername/Citrix/NFuse16>.

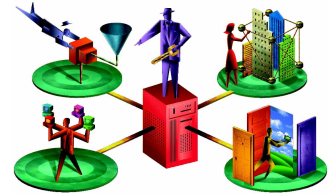
What to Do Next

If your users do not already have a supported ICA Client installed, they can use the Web-based ICA Client installation pages to download and install the appropriate ICA Client. See “Configuring Web-Based ICA Client Installation” on page 43 for more information.

For information about customizing your NFuse system, see the *Customizing NFuse Guide*, available as a PDF file in the \Doc directory on the NFuse CD-ROM.

For information about securing your NFuse system, see Chapter 5, “Configuring NFuse Security” on page 51.

Configuring ICA Client Devices



This chapter explains how to configure your ICA Client devices. To use an ICA Client device with NFuse, the device must have a supported Web browser and ICA Client installed. NFuse includes Web-based ICA Client installation to help you deploy and install ICA Clients. Web-based ICA Client installation uses HTML documents and ICA Client installation files stored on a Web server to determine the type of ICA Client supported by a device and to supply an appropriate ICA Client for installation.

Most ICA Clients require no configuration after installation to work with NFuse. However, two ICA Clients, the ICA Java Client and the ICA Macintosh Client, do require Web browser configuration. This chapter includes instructions for configuring the Web browsers of these ICA Clients.

Tasks to Complete

In this chapter you will:

- Learn about using Web-based ICA Client installation to deploy ICA Clients
- If necessary, configure the Web browsers of ICA Client devices

Configuring Web-Based ICA Client Installation

Web-based ICA Client installation is a default component of the installed Web sites. Included in each site are several files that aid in determining client device requirements and presenting installation files to users. In addition to automatic installation recommendations, the Web pages include installation links that users can click to manually invoke an ICA Client installation.

Note Citrix also provides a standalone version of Web-based ICA Client installation. You can use it to deploy ICA Clients independent of your NFuse Web sites. For more information, see the file Readme.htm in the NFuse CD-ROM's WebInst directory or in the downloaded CD image.

To use Web-based ICA Client installation you must make sure your Web server contains the ICA Client installation files.

ICA Client Installation Files

During Web Server Extension installation, the setup program prompts you to supply an ICA Client CD or CD image. Setup copies the contents of the CD's ICAWEB directory to a directory called /Citrix/ICAWEB that it creates off the Web server's Web publishing root directory. All included Web sites assume that the Web server contains the ICA Client files in the directory structure created by the Web Server Extension setup program:

<webroot>/Citrix/ICAWEB/<language>/<platform>

where *<webroot>* is your Web server's Web publishing root directory, *<language>* is the language version of the ICA Clients you want to deploy (en for English, de for German, fr for French, es for Spanish, or ja for Japanese), and *<platform>* is the Operating System type (ica16, ica32, icajava, icamac, icaunix, and icawince).

For example, in an English installation of the Web Server Extension on a typical Internet Information Server Web server, the ICA Win16 Client is contained in the following directory: C:\inetpub\WWWRoot\Citrix\ICAWEB\en\ICA16.

If you did not copy the ICA Client installation files to your Web server during Web Server Extension installation, make sure you copy the files to your Web server before using Web-based ICA Client installation.

► To copy the ICA Client files to your Web server

1. Create a directory called \Citrix\ICAWEB in your Web server's Web publishing root directory (usually C:\inetpub\WWWRoot).
2. Insert an ICA Client CD in your Web server's CD-ROM drive or browse your network for a shared ICA Client CD image.
3. Change directories to the CD's ICAWEB directory. Copy the contents of the ICAWEB directory on the CD into the /Citrix/ICAWEB directory on the server. Make sure you copy the contents of the directory and not the ICAWEB directory itself.

ICA Win32 Client Installation Files

By default, Web-based ICA Client installation offers 32-bit Windows client devices the ICA Win32 Web Client installation file. You can modify this behavior so that Web-based ICA Client installation offers the ICA Win32 Program Neighborhood Client or Program Neighborhood Agent for installation. The following list differentiates the three installation archives:

- **ICA Win32 Web Client installation file (Ica32t.exe).** The default archive for Web-based ICA Client installation, ICA32t.exe installs all files necessary for the ICA Win32 Client to launch and embed ICA sessions in Web browsers. This archive does not install the Program Neighborhood user interface and various other ICA Client components and is therefore smaller than the full archive and easier to download.
- **ICA Win32 Program Neighborhood Client installation file (Ica32.exe).** This archive installs all components of the ICA Win32 Client including the Program Neighborhood user interface. You must use this archive to install the ICA Win32 Client if your users require full ICA Client functionality.
- **ICA Win32 Program Neighborhood Agent installation file (Ica32a.exe).** This file installs all components of the ICA Win32 Client including the Program Neighborhood Agent user interface. You must use this file to allow your users to access NFuse-enabled published applications directly from the Windows desktop, Start menu, or in the Windows System Tray.

To change NFuse to offer a different ICA Client, edit the **Win32Client** parameter in the NFuse.conf file. After editing this file, you must restart your Web server.

Configuring Web Browsers

Before accessing published applications, some client devices must be configured for use with NFuse. Most supported ICA Clients require no additional configuration; however, the ICA Java Client (run in application mode) and the ICA Macintosh Client require configuration of the client device's Web browser before the ICA Client can be used with NFuse. When using these ICA Clients, you must manually register application/x-ica as a MIME type in the client device's browser.

Although the method differs slightly for each ICA Client/Web browser combination, in general, all browsers require the following information about the application/x-ica MIME type:

Field	Setting
File type	ICA
MIME type	application/x-ica
Description	ICA File
Extension	.ica
Helper Application	The location and name of the client device's ICA Client

The following procedures describe how to register application/x-ica as a MIME type on four ICA Client/Web browser combinations. For information about how to register MIME types on other supported browsers, see your browser's documentation.

Configuring the ICA Java Client

The following procedures describe how to configure the browser on an ICA Client device to associate the ICA Java Client with the application/x-ica MIME type. If you are running the ICA Java Client in applet mode, you do not need to configure the browser.

Note The following instructions describe how to configure Netscape Navigator Version 4.72 and Internet Explorer Version 4.5 for use with the ICA Java Client Version 4.11. For specific details about how to register a MIME type on other versions, see your browser's documentation.

- ▶ **To register application/x-ica as a Netscape Navigator MIME type**
 1. Install the ICA Java Client on the client device.
 2. Start Netscape Navigator.
 3. From the toolbar, select **Edit**, then **Preferences**. Under **Navigator**, select **Application**.
 4. Click the **New Type** button.
 5. In the **Description** field, type **ICA file**.
 6. In the **File extension** field, type **.ica**.
 7. In the **MIME type** field, type **application/x-ica**.

8. In the **Application to use** field, type `x:\jicasession.bat %1`, where *x* is the full path to `jicasession.bat`.
9. Click **OK**.

► **To register application/x-ica as an Internet Explorer MIME type on Win32 operating systems**

1. Log on to the client computer as an administrator.
2. Install the ICA Java Client on the client device.
3. On the client device, open a text editor and create the following .Reg file.

```
REGEDIT4
[HKEY_CLASSES_ROOT\MIME\Database\Content
Type\application/x-ica]
"Extension"=".ica"
```

4. Save this file as *yourfile.reg*.
5. Double click the .Reg file to update the client device's registry.

► **To associate .ica files with the ICA Client engine on Win32 operating systems**

1. Dbl click My Computer
2. Select the "Tools\Folder Options" menu
3. Click the "File Types" tab
4. Click New
5. Enter ICA as the File Extension
6. Click the "Change" button next to "Opens with"
7. Click "Other..."
8. Navigate to your Java Client installation directory and select
9. `jicasession.bat`
10. Click OK and then Close.

Configuring the ICA Macintosh Client

The following procedures describe how to configure the browser on a Macintosh to associate the ICA Macintosh Client with the application/x-ica MIME type.

Note The following instructions describe how to configure Netscape Navigator Version 4.72 and Internet Explorer Version 4.5 for use with the ICA Macintosh Client. For specific details about how to register a MIME type on other versions, see your browser's documentation.

► **To register application/x-ica as a Netscape Navigator MIME type**

1. Install the ICA Macintosh Client on the client device.
2. Start Netscape Navigator.
3. From the toolbar, select **Edit**, then **Preferences**. Under **Navigator**, select **Applications**.
4. Click the **New** button.
5. In the **Description** field, type **ICA file**.
6. In the **MIME Type** field, type **application/x-ica**.
7. In the **Suffixes** field, type **.ica**.
8. Select the **Application** radio button and click **Choose** to browse to the location of the ICA Macintosh Client.
9. Click **OK**.

► **To register application/x-ica as an Internet Explorer MIME type**

1. Install the ICA Macintosh Client on the client device.
2. Select **Edit**, then **Preferences**.
3. In the left panel of the **Preferences** dialog box, under **Receiving Files**, select **File Helpers**.
4. Click **Add** to display the **Edit File Helper** dialog box.
5. In the **Description** field, type **ICA file**.
6. In the **Extension** field, type **.ica**.
7. In the **MIME type** field, type **application/x-ica**.
8. In the **File Type** section of the dialog box, click **Browse**.
9. Browse to the location of the ICA Macintosh Client, select the ICA Client application, and click **Open**.

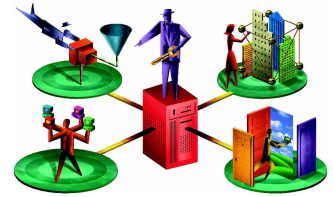
10. Select the **Binary data** radio button and **Use for Incoming** check box.
11. Select **Post process with Application** from the **How to Handle** drop down list.
12. Click **OK**.

What to Do Next

When you have installed and configured your ICA Client devices, NFuse setup is complete. For users to access the NFuse Web pages and their own application sets, provide them with the URL where your Web pages are saved.

For information about securing ICA Client devices, see Chapter 5, “Configuring NFuse Security” on page 51.

Configuring NFuse Security



This chapter includes information about how to secure your data in an NFuse environment. A comprehensive security plan must include the protection of your data at all points in the application delivery process. This chapter describes NFuse security risks and recommendations for each of the major NFuse communication links:

- **ICA Client Device — NFuse Web Server Communication.** Explains risks associated with passing NFuse data between Web browsers and Web servers and suggests strategies for protecting data in transit and data written on client devices.
- **NFuse Web Server — Citrix Server Communication.** Describes how to secure the authentication and published application information that passes between the NFuse Web server and your Citrix server farm.
- **ICA Client — Citrix Server Communication.** Explains risks associated with passing ICA session information between ICA Clients and Citrix servers and discusses implementation of NFuse and MetaFrame security features that protect such data.

ICA Client Device — NFuse Web Server Communication

NFuse communication between ICA Client devices and the NFuse Web server consists of passing several different types of data. As the user identifies himself, browses applications, and eventually selects an application to execute, the Web browser and Web server pass user credentials, application set lists, and session initializing files. Specifically, this network traffic includes:

- **HTML form data.** NFuse Web sites use a standard HTML form to transmit user credentials from the Web browser to the Web server at user logon time. The NFuse form passes the user name as clear text and uses only basic encryption for the domain name and password.

- **HTML cookies and pages.** After the user enters credentials in the NFuse Login page, the Web server writes the credentials in a transient cookie on the client device. The browser retransmits the cookie to the Web server with each HTTP GET request; for example, when the user browses applications in folders or whenever the user switches between pages in an NFuse Web site.

The HTML pages sent from the Web server to the browser contain application sets. These pages list the applications available to the user.

- **ICA files.** When the user selects an application, the Web server sends an ICA file for that application to the browser. The ICA file contains a ticket that can be used to log on to the MetaFrame server.

Risks

Attackers can exploit NFuse data as it crosses the network between the Web server and browser and as it is written on the client device itself:

- An attacker can intercept logon data, the credentials cookie, and HTML pages in transit between the Web server and Web browser.
- Although the credentials cookie used by NFuse is transient and disappears when the user closes the Web browser, an attacker with access to the client device's Web browser can retrieve the cookie and possibly steal credential information.
- Although the ICA file does not contain any user credentials, it contains a one-time use ticket that expires in 60 seconds. An attacker may be able to use the intercepted ICA file to connect to the MetaFrame server before the authorized user is able to use the ticket and make the connection.

Recommendations

The following recommendations combine industry-standard security practices with Citrix-provided safeguards to protect data travelling between client devices and your Web server and data written to client devices.

Implement SSL-Capable Web Servers and Web Browsers

Securing the Web server to Web browser component of NFuse communication begins with implementing secure Web servers and Web browsers. Many secure Web servers rely upon SSL technology to secure Web traffic.

In a typical Web server to Web browser transaction, the Web browser first verifies the identity of the Web server by checking the Web server's server certificate against a list of trusted certificate authorities. After verification, the Web browser encrypts user page requests and then decrypts the documents returned by the Web server. At each end of the transaction, Secure Socket Layer (SSL) message integrity checks ensure that the data has not been tampered with in transit.

In an NFuse deployment, SSL authentication and encryption creates a secure connection over which the user can pass credentials posted in the NFuse Login page. Data sent from the Web server, including the credentials cookie, ICA files, and HTML application list pages, is equally secure.

To implement SSL technology on your network, you must have an SSL-capable Web server and SSL-capable Web browsers. The use of these products is transparent to NFuse. No NFuse-specific configuration of your Web servers or browsers must be completed. For information about configuring your Web server to support SSL, see your Web server's documentation.

Important Many SSL-capable Web servers use TCP/IP port 443 for HTTP communications. By default, the Citrix SSL Relay uses this port as well. If your Web server is also a Citrix server running the SSL Relay, make sure you configure either the Web server or SSL Relay to use an alternate port.

NFuse Web Server — Citrix Server Communication

Communication between the Web server and Citrix server in an NFuse deployment involves passing user credential and application set information between the NFuse Java objects on the Web server and the Citrix XML Service in the Citrix server farm. In a typical NFuse session, the Java objects pass credentials to the XML Service for user authentication and the XML Service returns application set information. The Web server and server farm use a TCP/IP connection and the NFuse XML protocol to pass the information.

Risks

The NFuse XML protocol uses clear text to exchange all data with the exception of passwords, which it passes using Basic encryption. The XML communication is vulnerable to the following attacks:

- An attacker can intercept the XML traffic and steal application set information and tickets. An attacker with the ability to crack Basic encryption can obtain user credentials as well.
- An attacker can impersonate the Citrix server and intercept authentication requests.

Recommendations

Citrix recommends implementing one of the following security measures for securing the XML traffic between your Web server and Citrix server farm:

- Use the Citrix SSL Relay as a security intermediary between the Web server and Citrix server farm.
- In deployments that do not support running the SSL Relay, run the NFuse Web server on your Citrix server.

Use the Citrix SSL Relay

The Citrix SSL Relay is a MetaFrame component that uses SSL to secure communication between NFuse Web servers and Citrix server farms. The SSL Relay provides Citrix server authentication, data encryption, and message integrity for a TCP/IP connection.

The SSL Relay operates as an intermediary in the communication between the NFuse Web server and Citrix XML service. When using the SSL Relay, the Web server first verifies the identity of the SSL Relay by checking the Relay's server certificate against a list of trusted certificate authorities. After this authentication, the Web server and SSL Relay negotiate an encryption method for the session. The Web server can then send all information requests in encrypted form to the SSL Relay. The SSL Relay decrypts the requests and passes them to the Citrix XML service. When returning the information to the Web server, the Citrix server sends all information through the SSL Relay server, which encrypts the data and forwards it to the Web server for decryption. Message integrity checks verify each communication has not been tampered with.

Configuring NFuse to Use the Citrix SSL Relay

The SSL Relay is a default component of MetaFrame XP. On MetaFrame 1.8 servers, you must install Citrix MetaFrame 1.8 Service Pack 2 to use the SSL Relay. On MetaFrame 1.1 for UNIX, you must install Feature Release 1 to use the SSL Relay. In addition, each MetaFrame 1.8 or MetaFrame for UNIX server must have an installed and activated Feature Release 1 license. Make sure your Feature Release license is installed and activated on each server.

On the Citrix server side, using the SSL Relay to secure NFuse communication requires installation of a server certificate on the SSL Relay server and verification of the SSL Relay server's configuration. For information about installing a server certificate and configuring the SSL Relay on MetaFrame XP servers, see the installation chapter of the *MetaFrame XP Administrator's Guide*. For MetaFrame 1.8 servers, see the *Feature Release 1 and Service Pack 2 Installation Guide for Citrix MetaFrame for Windows Version 1.8*. On either platform, you can also consult the application help in the Citrix SSL Relay Configuration Tool.

When configuring the SSL Relay, make sure your Relay server permits passing SSL traffic to the Citrix servers you are using as the XML Service contacts. By default, the SSL Relay forwards traffic only to the server on which it is installed. You can, however, configure the SSL Relay to forward traffic to other servers. If the SSL Relay in your deployment is on a machine other than the machine to which you want to send NFuse data, make sure the SSL Relay's server list contains the server to which you want to forward NFuse data.

On the Web server side, you must change three parameters in the NFuse.conf file:

- **SessionField.NFuse_RelayServer** - Change to the name of a MetaFrame server running a properly configured SSL Relay.
- **SessionField.NFuse_RelayServerPort** - Change to the port number of the SSL Relay on the server specified in **SessionField.NFuse_RelayServer**.
- **SessionField.NFuse_Transport** - Change the value to "SSL."

Remember to restart the Web server after editing NFuse.conf.

Adding Certificates to the Web Server Extension

Citrix NFuse includes native support for the following certificate authorities:

- VeriSign, Inc., <http://www.verisign.com>
- Baltimore Technologies, <http://www.baltimore.com>

If you want to add support for other certificate authorities, you must add the certificate authority's root certificate to the Web Server Extension.

► To add a new root certificate to your Web Server Extension

1. Make sure the root certificate is in DER format.
2. Copy the root certificate to the following directory on your Web server:
 %SystemRoot%\keystore\cacerts by default on Windows Web servers
 /keystore/cacerts by default on UNIX Web servers

For information about certificates, see the installation chapter of the *MetaFrame Administrator's Guide* or the *Feature Release 1 and Service Pack 2 Installation Guide for Citrix MetaFrame for Windows Version 1.8*.

Running the NFuse Web Server on Your Citrix Server

For those deployments that do not support SSL Relay, the possibility of network attack can be eliminated by running a Web server on the Citrix server supplying the NFuse data. Hosting your NFuse Web sites on such a Web server routes all NFuse requests to the Citrix XML Service on the local host, thereby eliminating transmission of NFuse data across the network. Notice that the benefit of eliminating network transmission must be weighed against the risk of exploitation of the Web server.

In this deployment scenario, make sure your Web server and the Citrix XML Service operate on different TCP/IP ports. If you choose to use a non-default port for the Citrix XML Service, make sure you modify your Web pages to contact the local host on the non-default port.

Note On MetaFrame XP systems, the MetaFrame Setup routine lets you force the Citrix XML Service to share Internet Information Server's TCP/IP port instead of using a dedicated port. If you have enabled port sharing, the XML Service and the Web server use the same port by default.

At minimum, you can place both your Web server and Citrix server behind a firewall so that the communication between the two is not exposed to open Internet conditions. In this scenario, client devices must be able to communicate through the firewall to both the Web server and Citrix server. Your firewall must permit HTTP traffic (often over the standard HTTP port 80 or 443 if a secure Web server is in use) for client device to Web server communication. For ICA Client to Citrix server communication, the firewall must permit inbound ICA traffic on port 1494 and outbound traffic on a dynamically generated port above 1023. See your server documentation for information about using ICA with network firewalls.

For information about using NFuse with network address translation, see “NFuse’s Server Location Options” in the NFuse SDK. This topic includes information about server location through firewalls.

ICA Client — Citrix Server Communication

NFuse communication between client devices and Citrix servers consists of passing several different types of ICA session data including initialization requests and ICA session information.

- **Initialization requests.** The first step in establishing an ICA session, called *initialization*, requires the ICA Client to request an ICA session and produce a list of ICA session configuration parameters that control various aspects of the ICA session such as the user to log on, the size of the window to draw, and the program to execute in the session.
- **ICA session information.** After session initialization, the ICA Client passes user keyboard and mouse input to the Citrix server as the user navigates the chosen application. In response, the Citrix server sends the ICA Client graphical updates.

Risks

To capture and interpret ICA Client to Citrix server network communications, an attacker must be able to crack the binary ICA protocol. An attacker with binary ICA protocol knowledge can:

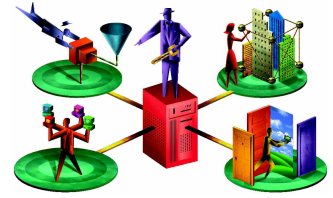
- Intercept initialization request information sent from the ICA Client, including user credentials.
- Intercept ICA session information including text and mouse clicks entered by users and screen updates sent from the Citrix server.

Recommendations

Citrix recommends implementing SSL or SecureICA encryption to secure the traffic between your ICA Clients and Citrix servers. Both methods support 128-bit encryption of the data stream between the ICA Client and MetaFrame server, but SSL also supports verification of the identity of the MetaFrame server.

Support for SSL is included in Feature Release 1 for MetaFrame XP and Feature Release 1 for MetaFrame for UNIX. Support for SecureICA is included in Feature Release 1 for MetaFrame 1.8 and MetaFrame XP. Please see your ICA Client documentation or the Citrix download site for a list of ICA Clients that support each method. See the *MetaFrame Administrator's Guide* for MetaFrame 1.8 and MetaFrame XP for more information on SecureICA.

ICA Program Neighborhood Agent Configuration



The ICA Win32 Program Neighborhood Agent is configured with default presentation options, authentication methods, and server connection options. You can change these defaults and prevent users from changing specific options by editing the Config.xml file located in the wwwroot\Citrix\PNAgent directory on the NFuse Web server.

The Config.xml file contains a number of parameters divided into eight categories:

- FolderDisplay - Specifies whether to display application icons in the Start menu, on the Windows desktop, and in the system tray. There are also additional parameters to specify a specific folder in the Start menu and the icon to use on the Windows desktop. Corresponds to the options on the **Application Display** tab of the **PN Agent Properties** dialog box.
- DesktopIntegration - Do not edit.
- Configuration File - Allows you to specify a different URL for Config.xml that the client should use in the future. This facilitates moving users to a different NFuse server.
- Request - Specifies where the client should request published application data from, and how often to refresh the information.
- Logon - Specifies the logon method to use.
- UserInterface - Specifies whether to hide or display certain groups of options presented to the user as part of the Program Neighborhood Agent interface.
- FileCleanup - Do not edit.
- ICA_Options - Specifies the audio and video options for ICA connections. Corresponds to the options on the **ICA Options** tab of the **PN Agent Properties** dialog box.

Not all of the above groups are included in the Config.xml file by default. Only three parameters are actually required in Config.xml: Request/Enumeration/Location, Logon/LogonMethod, and Logon/SupportNDS. Default values are used for parameters that are not specified. Some parameters, if specified, have child parameters that must also be specified. In the table below, any required child parameters are listed in the description for the parent parameter.

All parameters that can be edited by users through the **PN Agent Properties** dialog box have two attributes: **modifiable** and **forcedefault**. Each attribute can either be true or false. If the **modifiable** attribute is true, users can change the value using the **PN Agent Properties** dialog box. If the **forcedefault** attribute is true, the Program Neighborhood Agent setting is reset to the value specified in the Config.xml file each time the Program Neighborhood Agent is run. If **modifiable** is set to true, **forcedefault** should be set to false.

The following table describes each parameter.

Parameter	Default Value (Value Type)	User-Editable	Description
FolderDisplay/StartMenuDisplay/Enabled	true	Yes	Adds shortcuts to remote applications in each user's Windows Start menu.
FolderDisplay/StartMenuDisplay/RootFolder	programs	Yes	The name of the folder to group remote applications into. If no name is specified, applications show up as individual icons in the Start menu folder. This parameter corresponds to the Show this folder in Programs submenu check box in the Application Display tab of the PN Agent Properties dialog box of the Program Neighborhood Agent. If the value is "programs", the box is checked. If the root parameter is not included in Config.xml, the box is not checked.
FolderDisplay/DesktopDisplay/Enabled	false	Yes	Include remote applications in a folder on the Windows desktop. This parameter corresponds to the Show applications in Start menu check box in the Application Display tab of the PN Agent Properties dialog box of the Program Neighborhood Agent.
FolderDisplay/DesktopDisplay/Icon/Name	Citrix Program Neighborhood	Yes	The name of the folder on the Windows desktop. This parameter corresponds to the Show applications in Start menu text-entry box in the Application Display tab of the PN Agent Properties dialog box of the Program Neighborhood Agent.

Parameter	Default Value (Value Type)	User-Editable	Description
FolderDisplay/DesktopDisplay/Icon/Location	(URL)	No	Location of file containing icon to use for desktop folder. If no location is specified, the default Program Neighborhood Agent icon is used.
FolderDisplay/SystemTrayMenuDisplay/Enabled	true	Yes	Display published applications in the pop-up menu for the Program Neighborhood Agent system tray icon. This parameter corresponds to the Display applications in System Tray check box in the Application Display tab of the PN Agent Properties dialog box of the Program Neighborhood Agent.
ConfigurationFile/Location	http:// servername/ Citrix/ PNAgent/ config.xml	Yes	The URL to request configuration data This parameter corresponds to the Server URL box in the Server tab of the PN Agent Properties dialog box of the Program Neighborhood Agent.
ConfigurationFile/Refresh/Poll/Enabled	false	No	An option to have the configuration data updated on a poll mechanism.
ConfigurationFile/Refresh/Poll/Period	8	No	The period in hours to refresh the configuration information.
Request/Enumeration/Location	http:// servername/ Citrix/ PNAgent/ enum.asp	No	The URL for the enum.asp or enum.jsp file on the NFuse Web server.
Request/Enumeration/Refresh/OnApplicationStart	true	Yes	Refresh published application data when Program Neighborhood Agent is run. This parameter corresponds to the Refresh list when PN Agent starts box in the Application Refresh tab of the PN Agent Properties dialog box of the Program Neighborhood Agent.
Request/Enumeration/Refresh/OnResourceRequest	false	Yes	Refresh published application data when a published application is run. This parameter corresponds to the Refresh list when remote application launched box in the Application Refresh tab of the PN Agent Properties dialog box of the Program Neighborhood Agent.

Parameter	Default Value (Value Type)	User- Editable	Description
Request/Enumeration/Refresh/ Poll/Enabled	true	Yes	Refresh enumeration on a timed interval. This parameter corresponds to the Refresh list on hourly interval check box in the Application Refresh tab of the PN Agent Properties dialog box of the Program Neighborhood Agent. Note: forcedefault and modifiable attributes are on Request/Enumeration/Refresh/Poll.
Request/Enumeration/Refresh/ Poll/Period	6	Yes	If Request/Enumeration/Refresh/Poll/Enabled is true, this parameter specifies the interval, in hours, at which published application data is refreshed. This parameter corresponds to the Refresh list on hourly interval text entry box in the Application Refresh tab of the PN Agent Properties dialog box of the Program Neighborhood Agent. Note: forcedefault and modifiable attributes are on Request/Enumeration/Refresh/Poll.
Request/Resource/Location	http:// <i>servername</i> / Citrix/ PNAgent/ enum.asp http:// <i>servername</i> / Citrix/ PNAgent/ launch.asp	No	The URL for the launch.asp or launch.jsp file on the NFuse Web server.
Logon/LogonMethod	sson prompt	No	The logon method to use. If "prompt", prompt for user name, password, and domain name. If "sson", use single sign-on credentials. If "anonymous", don't prompt for user credentials. Instead, authenticate as an anonymous user.
Logon/SupportNDS	false	No	Specifies whether to use NDS authentication. If true, you must also define Logon/NDS_Settings/DefaultTree .
Logon/NDS_Settings/DefaultTree	N/A	No	When using NDS authentication, this parameter specifies the NDS tree to use for authenticating users.

Parameter	Default Value (Value Type)	User- Editable	Description
UserInterface/ServerSettings	true	No	Specifies whether to display the Server tab in the PN Agent Properties dialog box on client computers.
UserInterface/ FolderDisplaySettings	true	No	Specifies whether to display the Application Display tab in the PN Agent Properties dialog box on client computers.
UserInterface/RefreshSettings	false	No	Specifies whether to display the Application Refresh tab in the PN Agent Properties dialog box on client computers.
ICA_Options/DisplaySize/Value/ Percent	(1-100)	No	Specifies a size for ICA session windows as a percentage of the total screen size on the client computer.
ICA_Options/DisplaySize/Value/ Dimension/Height	(NUMBER)	No	Specifies the height for ICA session windows in pixels.
ICA_Options/DisplaySize/Value/ Dimension/Width	(NUMBER)	No	Specifies the width for ICA session windows in pixels.
ICA_Options/DisplaySize/Value/ Mode	seamless fullscreen	No	Specifies the ICA connection types to make available to users in the ICA Options tab of the PN Agent Properties dialog. Each value must be specified separately. If "seamless", allow seamless connections. If "fullscreen" allow full-screen ICA sessions.
ICA_Options/ColorDepth/Options	1 2 4 8	No	Specifies the color depths to make available to users in the ICA Options tab of the PN Agent Properties dialog according to the following table: 1 - 16 colors 2 - 256 colors 4 - High color (16 bit) 8 - True color (24 bit) Each value must be specified separately.
ICA_Options/Audio/Options	high medium low off	No	Specifies the audio quality options to make available to users in the ICA Options tab of the PN Agent Properties dialog. Each value must be specified separately.

Securing the Program Neighborhood Agent With SSL

To use SSL to secure the communications between the Program Neighborhood Agent and the NFuse Web server, change the URLs in the following parameters in the Config.xml file to use HTTPS. Not all parameters may be specified in your version of the file.

- FolderDisplay/DesktopDisplay/Icon/Location
- ConfigurationFile/Location
- Request/Enumeration/Location
- Request/Resource/Location

Example: If the line specifying Request/Resource/Location is `<Location>http://server3.eng.citrix.com/Citrix/PNAgent/launch.asp</Location>`, change it to `<Location>https://server3.eng.citrix.com/Citrix/PNAgent/launch.asp</Location>`

To secure the connection between the Program Neighborhood Agent and the MetaFrame server using SSL, follow the instructions in this book for configuring NFuse to use SSL and check the **Enable SSL** box in the **ICA Client Options** tab of the application properties dialog box in the Citrix Management Console.

Index

A

- Apache Server
 - installing Web Server Extension 28
- application publishing 12
- application set 12

C

- CDN 7
- Citrix Developer Network 7
- Citrix XML Service 12
- Config.xml 59

D

- documentation 6
 - reader response 8

F

- firewalls 56
- functional overview of NFuse 15

I

- ICA Client device 13
- ICA Clients
 - Java
 - configuring 46
 - Macintosh (configuring) 48
 - required configuration 45
 - Web-based ICA Client installation
 - using to deploy ICA Clients 43
- ICA files 16
- ICA Win32 Program Neighborhood Agent
 - configuring 59
- installing
 - Web Server Extension
 - on IIS 26
- Internet Explorer
 - using with the ICA Java Client 47
 - using with the ICA Macintosh Client 48
- Internet Information Server
 - installing Web Server Extension 26
 - requirements 18

iPlanet Web Server

- configuring the Web Server Extension 31
- installing Web Server Extension 28

M

- MetaFrame for UNIX Operating Systems
 - determining XML Service port 25, 30
 - requirements 16
 - role in NFuse 12
- MIME type
 - configuring for ICA Java Client 46
 - configuring for ICA Macintosh Client 48

N

- Netscape Navigator
 - using with the ICA Java Client 46
 - using with the ICA Macintosh Client 48
- NFuse.properties
 - description and contents 34

O

- override order of session fields 36

P

- PNAgent
 - see Program Neighborhood Agent 59
- Program Neighborhood Agent
 - configuring 59

R

- requirements
 - Citrix server 16
 - ICA Client device 20
 - Web server 18

S

- secure Web servers 52
- SecureICA 57

security

network communication

between client device and Web server 51

between ICA Client and Citrix server 57

between Web server and Citrix server 53

SSL

adding certificates 55

between Web server and Citrix server 54

between Web server and Web browser 52

configuring NFuse to use the SSL Relay 55

configuring the SSL Relay 54

session fields

precedence 36

Solaris

configuring the Web Server Extension 31

SSL

configuring the SSL Relay 54

finding more information on the SSL Relay 6–7

secure Web servers 52

using the SSL Relay 54

W

Web browsers

required configuration 45

Web server

role in NFuse system 13

security 52

Web Server Extension

configuring properties 34

files copied to Web server 28

installing on Apache, Netscape, and iPlanet 28

installing on IIS 26

Web-based ICA Client installation

copying ICA Clients to your Web server 44

introduction 43

X

XML Service 12

determining port in use on Citrix server 25