

Administrator's Guide

Citrix NFuse™ Classic

Version 1.7

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.

© 2000-2002 Citrix Systems, Inc. All rights reserved.

Citrix, MetaFrame, Program Neighborhood, and ICA are registered trademarks, and SecureICA and NFuse 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 Java Edition, © 1999, 2000 IBM Corporation.

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

Contents

Chapter 1 Introduction.....	7
Overview	7
How to Use This Guide	8
Document Conventions	8
Finding More Information	9
Using PDF Documentation.....	10
Reader Comments	10
Citrix on the World Wide Web	11
Introducing Citrix NFuse Classic.....	12
NFuse Classic Features	13
Manageability Features	13
Application Access Features	14
Security Features	14
Client Deployment Features.....	15
What's New in NFuse Classic 1.7.....	15
Manageability Features	15
Application Access Features	16
Security Features	17
Client Deployment Features.....	17
NFuse Classic Components	18
MetaFrame Server Farm.....	18
Web Server.....	19
ICA Client Device	19
How NFuse Classic Works	20
What to Do Next.....	22
Chapter 2 Deploying NFuse Classic	23
Overview	23
System Requirements.....	24
MetaFrame Server Requirements	24
Supported MetaFrame Versions.....	24
Additional Software Requirements	24
General Configuration Requirements.....	26
Backward Compatibility.....	26
Web Server Requirements	27
On Windows Platforms	27

On UNIX Platforms	27
ICA Client Device Requirements	28
Installing NFuse Classic	30
Installation Overview	30
Installing NFuse Classic During MetaFrame XP Installation	30
Installing NFuse Classic Separately from MetaFrame XP	30
Upgrading an Existing Installation	31
What Is Installed Where?	32
Security Considerations	33
Required Information	33
Installing NFuse Classic on Microsoft IIS	35
Installing NFuse Classic on UNIX Platforms	36
File Location Information	37
Configuring Your Web Server for NFuse Classic	39
Configuring iPlanet Web Server	39
Configuring WebSphere Web Server	39
What to Do Next	41
Troubleshooting NFuse Classic Installation	42
Using the Repair Option	42
Uninstalling NFuse Classic	43
Uninstalling NFuse Classic on Microsoft IIS	43
Uninstalling NFuse Classic on iPlanet, Tomcat, and WebSphere	44
Chapter 3 Configuring NFuse Classic	45
Overview	45
Deciding Which Configuration Method to Use	46
Configuring NFuse Classic Using the Administration Tool	47
Accessing the Admin Tool	47
Saving, Applying, and Discarding Changes	48
Getting Online Help	48
Configuring Communication With MetaFrame	49
Configuring Fault Tolerance	50
Enabling Load Balancing Between Servers	51
Specifying the TCP/IP Port for XML Communication	51
Specifying the Transport Protocol	52
Configuring Authentication	53
Authentication Recommendations	54
Configuring Explicit Authentication	55
Enabling Guest User Access	56
Enabling Desktop Credential Pass-Through (Single Sign On)	57
Enabling Smart Card Authentication	60

Configuring Ticket Expiry Time	63
Examples	63
Configuring Address Translation.....	66
About Address Translation.....	66
Specifying the Default Behavior	67
Configuring Specific Address Translation Settings.....	68
Defining Address Translation Mappings	69
Examples	70
Configuring Citrix Secure Gateway Support.....	74
Example	76
Configuring Client-Side Firewall Settings	77
Example	79
Allowing Users to Configure NFuse Classic Settings.....	80
How User Settings are Stored on Client Devices.....	81
Configuring ICA Client Deployment	82
Configuring Web-Based ICA Client Installation.....	83
Controlling the Launching and Embedding of Applications	85
Customizing ICA Java Client Deployment	87
Configuring Communication With Enterprise Services for NFuse	89
Changes to NFuse Classic Features	89
Configuring NFuse Classic Using NFuse.conf	91
Examples	105
Configuring Communication with MetaFrame	105
Configuring SSL Relay Communication	105
Configuring Citrix Secure Gateway Support	106
Making NFuse Classic Available to Users	107
Making the Login Page the Default Web Page	107
What to Do Next.....	107
Chapter 4 ICA Clients and NFuse Classic.....	109
Overview	109
About Web-Based ICA Client Installation	110
Copying ICA Client Installation Files to your Web Server	110
Configuring Web-Based ICA Client Installation	111
ICA Win32 Client Installation Files.....	111
Configuring Installation Captions	112
About the ICA Java Client.....	113
About the ICA Win32 Program Neighborhood Agent	114
Configuring the ICA Macintosh Client	115
Registering Application/x-ica as a MIME Type	115
What to Do Next.....	116

Chapter 5	Configuring NFuse Classic Security	117
Overview		117
Introduction		118
About Security Protocols and Citrix Security Solutions		119
SSL		119
TLS		119
Citrix SSL Relay		120
ICA Encryption (Citrix SecureICA)		120
Citrix Secure Gateway		121
ICA Client Device—NFuse Classic Server Communication		122
Risks		122
Recommendations		123
Implement SSL/TLS-Capable Web Servers and Web Browsers		123
Do Not Enable Pass-through Authentication		123
NFuse Classic Server—MetaFrame Server Communication		124
Risks		124
Recommendations		124
Use Citrix SSL Relay		124
Run the NFuse Classic Server on Your MetaFrame Server		126
Use the HTTPS Protocol		127
ICA Client—MetaFrame Server Communication		128
Risks		128
Recommendations		128
Use SSL/TLS or ICA Encryption		128
Use Citrix Secure Gateway		129
General Security Considerations		129
Index		131

Introduction



Overview

Welcome to Citrix NFuse Classic, Version 1.7. This chapter introduces you to the documentation and to NFuse Classic. Topics include:

- How to use this guide
- An introduction to NFuse Classic and its components
- What's new in NFuse Classic 1.7

How to Use This Guide

The *Citrix NFuse Classic Administrator's Guide* is for MetaFrame server administrators and Web masters responsible for installing, configuring, and maintaining NFuse Classic.

This is a task-based guide to help you set up NFuse Classic quickly and easily. This chapter introduces the documentation and the Citrix NFuse Classic product, and describes what's new in this version. Subsequent chapters explain how to deploy and configure NFuse Classic in your MetaFrame installation.

This guide assumes knowledge of Citrix MetaFrame for Windows or Citrix MetaFrame for UNIX Operating Systems.

Document Conventions

The following conventional terms, text formats, and symbols are used throughout the printed documentation:

Convention	Meaning
Boldface	Commands, names of interface items such as text boxes and option buttons, and user input.
<i>Italics</i>	Placeholders for information or parameters that you provide. For example, <i>filename</i> in a procedure means you type the actual name of a file. Italics also are used for new terms and the titles of books.
UPPERCASE	Keyboard keys, such as CTRL for the Control key and F2 for the function key that is labeled F2.
Monospace	Text displayed at a command prompt or in a text file.
%SystemRoot%	The Windows system directory, which can be WTSRV, WINNT, WINDOWS, or other name specified when Windows is installed.
{ braces }	A series of items, one of which is required in command statements. For example, { yes no } means you must type yes or no . Do not type the braces themselves.
[brackets]	Optional items in command statements. For example, [/ping] means that you can type /ping with the command. Do not type the brackets themselves.
(vertical bar)	A separator between items in braces or brackets in command statements. For example, { /hold /release /delete } means you type /hold or /release or /delete.
... (ellipsis)	You can repeat the previous item or items in command statements. For example, /route:devicename[...] means you can type additional devicenames separated by commas.

Finding More Information

NFuse Classic includes the following documentation:

- The *Citrix NFuse Classic Administrator's Guide* (this document) introduces NFuse Classic and explains how to install NFuse Classic and configure your NFuse server, ICA Client devices, and security. This guide is on the Components CD-ROM and on the Citrix Web site (<http://www.citrix.com/support>). Select Product Documentation.
- Online help for the NFuse Classic Administration tool. To access the NFuse Classic Admin tool help system, click the **Help** link that is available in all the pages. The help is displayed in a new browser window.
- The *Customizing NFuse Classic* guide explains how to customize NFuse Classic. This guide is on the Components CD-ROM and on the Citrix Web site (<http://www.citrix.com/support/>). Select Product Documentation.
- The NFuse Classic Readme file contains last minute updates, corrections to the documentation, and a list of known problems. This file is on the Components CD-ROM and on the Citrix Web site (<http://www.citrix.com/support/>). Select Product Documentation.

Other sources of information about NFuse Classic and Citrix products:

- The *Citrix MetaFrame XP for Windows, Version 1.0, Feature Release 2 Administrator's Guide* explains how to install and configure MetaFrame XP Feature Release 2 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 on the MetaFrame XP CD-ROM and on the Citrix Web site.
- 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 Web 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 configuring the XML Service for UNIX. The *MetaFrame for UNIX Administrator's Guide* is available on the MetaFrame for UNIX, Feature Release 1 CD-ROM and on the Citrix Web site.

- The *Citrix SSL Relay for UNIX Administrator's Guide* is for system administrators who are responsible for installing, configuring, and maintaining Citrix SSL Relay on MetaFrame for UNIX Operating Systems servers. This guide is available on the MetaFrame for UNIX Feature Release 1 CD-ROM and on the Citrix Web site.
- The *Citrix Enterprise Services for NFuse Administrator's Guide Version 1.7* tells administrators how to install and configure Enterprise Services for NFuse. This guide is on the Components CD-ROM and on the Citrix Web site.
- The *Citrix Secure Gateway Administrator's Guide Version 1.1* tells administrators how to install and configure Citrix Secure Gateway. This guide is on the Components CD-ROM and on the Citrix Web site.

Using PDF Documentation

To access the Citrix documentation that is provided in PDF files, use Adobe Acrobat Reader 4 or later. Acrobat Reader lets you view, search, and print the documentation. You can download Acrobat Reader for free from Adobe System's Web site (<http://www.adobe.com>). The self-extracting file includes installation instructions.

Reader Comments

We strive to provide accurate, clear, complete, and usable documentation for Citrix products. If you have any comments, corrections, or suggestions for improving our documentation, we want to hear from you. You can send e-mail to the documentation authors at:

documentation@citrix.com

Please include the product name and version number, and the title of the document in your message.

Citrix on the World Wide Web

The Citrix Web site is at <http://www.citrix.com>. The site offers a variety of information and services for Citrix customers and users.

From the Citrix home page, you can access Citrix technical support services and other information designed to assist MetaFrame XP administrators.

The following are some of the resources available on the Citrix Web site:

Citrix Product Documentation Library. The library, which contains the latest documentation for all Citrix products, is at <http://www.citrix.com/support> (select Product Documentation). You can download updated editions of the documentation that ships with Citrix products, as well as supplemental documentation that is available only on the Web site.

Citrix ICA Clients. Downloadable Citrix ICA Clients for all supported platforms are available from <http://www.citrix.com/download>.

Support options. Program information about Citrix Preferred Support Services options is available from the Support area of the Citrix Web site at <http://www.citrix.com/support>.

Software downloads. An FTP server provides access to the latest service packs, hotfixes, utilities, and product literature for download.

Online knowledge base. The online Solution Knowledge Base contains an extensive collection of application notes, technical articles, troubleshooting tips, and white papers.

Discussion forums. The interactive online Solution Forums provide outlets for discussion of technical issues with other Citrix users.

FAQs. Frequently Asked Questions (FAQ) pages provide answers to common technical and troubleshooting questions.

Education. Information about programs and courseware for Citrix training and certifications is available from <http://www.citrix.com/training/>.

Contact information. The Web site provides contact information for Citrix offices, including the worldwide headquarters and headquarters for European, Asia Pacific, and Japan operations.

Developer network. The Citrix Developer Network (CDN) is at <http://www.citrix.com/cdn>. This open-enrollment membership program provides access to developer toolkits, technical information, and test programs for software and hardware vendors, system integrators, ICA licensees, and corporate IT developers who incorporate Citrix computing solutions into their products.

Introducing Citrix NFuse Classic

NFuse Classic is a Web-based application deployment system that provides users with access to MetaFrame applications through a standard Web browser.

NFuse Classic employs Java object technology executed on a Web server to dynamically create an HTML-based depiction of the MetaFrame server farm for each of your users. Included in each user's presentation are all the applications published in the MetaFrame server farm for that user.

NFuse Classic offers the administrator the centralized application management capabilities that you'd expect of Citrix software, and places complete control over the application deployment process in the hands of the administrator. Using NFuse Classic, you can create standalone Web sites for application access or Web sites that can be integrated into your corporate portal.

An easy to use graphical user interface allows you to administer and configure NFuse Classic on the Windows platform. There is also a configuration file that lets you change many of NFuse Classic's properties. The *Citrix NFuse Classic Administrator's Guide* (this guide) explains how to use these tools.

In addition, NFuse Classic provides various mechanisms you can use to customize and extend NFuse Classic's capabilities. You can use Active Server Pages or JavaServer Pages to write Web server scripts that manipulate the NFuse Classic Java objects. Or, if you are unfamiliar with Web server scripting, you can use simplified Citrix substitution tags to access the NFuse Classic Java objects. You can also write your own Java servlets using the NFuse Classic Java objects. The *Customizing NFuse Classic* guide explains how to customize NFuse Classic using these methods.

Note NFuse has changed its name to NFuse Classic. However, this guide refers to both older versions of NFuse and the new NFuse Classic version.

NFuse Classic Features

This section provides information about NFuse Classic features. For details about which MetaFrame and ICA Client versions are required for particular NFuse Classic features, see “MetaFrame and ICA Client Version Requirements for NFuse Classic Features” on page 25.

Manageability 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 Classic’s Java objects can be accessed from Web server scripts, such as Microsoft’s Active Server Pages and Sun Microsystems’ JavaServer Pages.

Windows installer support NFuse Classic is available in a Windows Installer package (.msi-type file). The Windows Installer also provides Repair and Remove options.

NDS support. There is a separate NFuse Login page for NDS. This contains a context field that allows users to search for their user name in the tree to determine which context they are in. NDS authentication is supported on Windows IIS/ASP only.

Internet Server Application Program Interface (ISAPI) extension. The Citrix XML Service contains an ISAPI extension that you can plug into Internet Information Server (IIS). Plugging the XML Service into IIS allows IIS to handle NFuse Classic requests and serve NFuse Classic 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 Classic components are compatible with Microsoft Active Directory. Users visiting NFuse Classic Web pages can log on to a Citrix server farm that is part of an Active Directory deployment and seamlessly access Citrix published applications. The logon pages in NFuse Classic Web sites are now compatible with Active Directory’s use of User Principal Names.

Application Access Features

Support for MetaFrame for UNIX Operating Systems. Support for MetaFrame for UNIX Operating System server farms allows NFuse Classic to display and launch applications running on UNIX platforms on your users' client devices.

Citrix Enterprise Services for NFuse support Citrix Enterprise Services for NFuse extends the application management and deployment features of NFuse Classic to allow user access to applications provided by multiple MetaFrame farms.

Backup MetaFrame servers. You can configure backup MetaFrame servers to ensure that users still have access to their applications in the event of a server failure.

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

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

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

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

Security Features

Secure Sockets Layer (SSL) support. NFuse Classic supports SSL to secure communication between your Web server and Citrix server farm. SSL is an open, non-proprietary 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 Classic 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.

Citrix Secure Gateway support Citrix Secure Gateway, together with NFuse Classic provides a single, secure, encrypted point of access through the Internet to MetaFrame servers on your internal corporate networks. Citrix Secure Gateway simplifies certificate management, because a server certificate is required only on the Secure Gateway server, rather than on every MetaFrame server in the farm.

Ticketing. This feature provides enhanced authentication security. NFuse Classic 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 Classic uses to launch applications.

Client Deployment Features

Web-based ICA Client installation. You can use NFuse Classic to deploy ICA Clients to any device that has a Web browser. When a client device user visits an NFuse Classic 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.

ICA Win32 Program Neighborhood Agent support. The ICA Win32 Program Neighborhood Agent allows 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 from 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.

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

What's New in NFuse Classic 1.7

NFuse Classic 1.7 offers the following new features:

Manageability Features

Web-based Admin tool NFuse Classic provides a Web-based administration tool that allows you to perform day to day NFuse Classic administration tasks quickly and easily. For example, you can use the Admin tool to configure communication with MetaFrame servers running the Citrix XML Service, or to specify the settings that users can adjust on the Settings page. The Admin tool is available only on Windows/Internet Information Server (IIS) machines, and requires Internet Explorer Version 5.0 or later.

Enhanced NAT support You can configure different types of network address translation (NAT) using NFuse Classic. For example, you can specify default address translation behavior or configure settings for particular addresses, depending on the configuration of your firewall and MetaFrame server. You can also configure port address translation, which allows you to route traffic to internal MetaFrame servers through a single external IP address using several ports.

SOCKS proxy support If you are using a SOCKS proxy server at the client-side of your NFuse Classic installation, you can configure general SOCKS proxy rules for all clients, together with specific SOCKS proxy rules for particular clients.

Load balancing XML requests You can load balance connections between MetaFrame servers running the Citrix XML Service. Enabling load balancing allows you to evenly distribute connections among these servers so that no one server becomes overloaded.

Users can change their passwords You can configure NFuse Classic so that your users can change their logon password in an NFuse Classic session. You can allow users to change their password whenever they like, or only when it expires. You can also prevent users from changing their password.

Application Access Features

Desktop Credential Pass-Through (Single Sign On) Desktop Credential Pass-Through is a feature of Internet Explorer and IIS that allows users to authenticate to NFuse Classic using the credentials they provided when they logged on to their Windows desktop. When used in combination with pass-through authentication, a feature of the ICA Win32 Client, users log on only once, thereby eliminating the need to remember multiple sign on processes, user ids, and passwords. For this feature to work, NFuse Classic must be running on IIS and users must be running Internet Explorer Version 5.0 or later, on Windows 2000 or later.

Smart card support Users can authenticate to NFuse Classic by inserting a smart card in a smart card reader attached to the client device. Smart cards eliminate the need for users to remember multiple sign-on processes, user ids, and passwords. For this feature to work, NFuse Classic must be running on IIS and users must be running Internet Explorer Version 5.0 or later on Windows 2000 or later.

Launching and Embedding Applications You can control whether applications are launched from or embedded in HTML pages. If you embed applications, you can specify the ICA Client used to launch applications and configure the components included in the deployment of the ICA Java Client. You can also enable users to decide how their applications are launched.

Enhanced Content Publishing NFuse Classic supports the Enhanced Content Publishing features, available in Feature Release 2 for MetaFrame XP. Content Publishing allows you to associate content with a published application on a MetaFrame XP server. Previously, users could open published content only with locally installed player or viewer applications. Content Publishing now allows “browser only” devices that do not have locally installed applications to open content published on MetaFrame servers. This capability is supported only when users connect to published content through NFuse.

Note For applications to work with Enhanced Content Publishing, they must be capable of accepting command line arguments—for example, Notepad accepts UNC addresses but not URLs. For more information about this feature, see the *Citrix MetaFrame XP Feature Release 2 Administrator's Guide*.

Security Features

Transport Layer Security (TLS) Encryption NFuse Classic supports TLS, which is the latest, standardized version of the SSL protocol. TLS provides server authentication, encryption of the data stream, and message integrity checks. Note that the server certificates you use for SSL in your MetaFrame installation will also work with TLS.

Client Deployment Features

Automatic delivery of the ICA Win32 Web Client You can automatically deploy the ICA Win32 Web client installation file (Ica32t.exe) to your Windows users. This client does not install the Program Neighborhood user interface and various other ICA Client components. Therefore, this client is smaller and easier to download than the full client, so is suitable for users on low bandwidth connections.

NFuse Classic Components

An NFuse Classic deployment involves the interaction of three network components:

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

MetaFrame Server Farm

A MetaFrame *server farm* is a group of MetaFrame 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. MetaFrame 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 on 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 Classic system, the NFuse Classic server functions as a Web-based Program Neighborhood interface for connecting to a MetaFrame server farm. The NFuse Classic 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 MetaFrame server farm, the NFuse Classic 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 Classic servers using TCP/IP. This service functions as the contact point between the server farm and NFuse Classic server. 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 Classic system hosts the NFuse Classic Java objects and Web server-side scripts. The NFuse Classic Java objects provide the following services:

- Authenticate users to a MetaFrame 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 Classic Java objects are added to your Web server during NFuse Classic installation. This installation program also adds Web pages and configuration files.

ICA Client Device

In the context of NFuse Classic, 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.

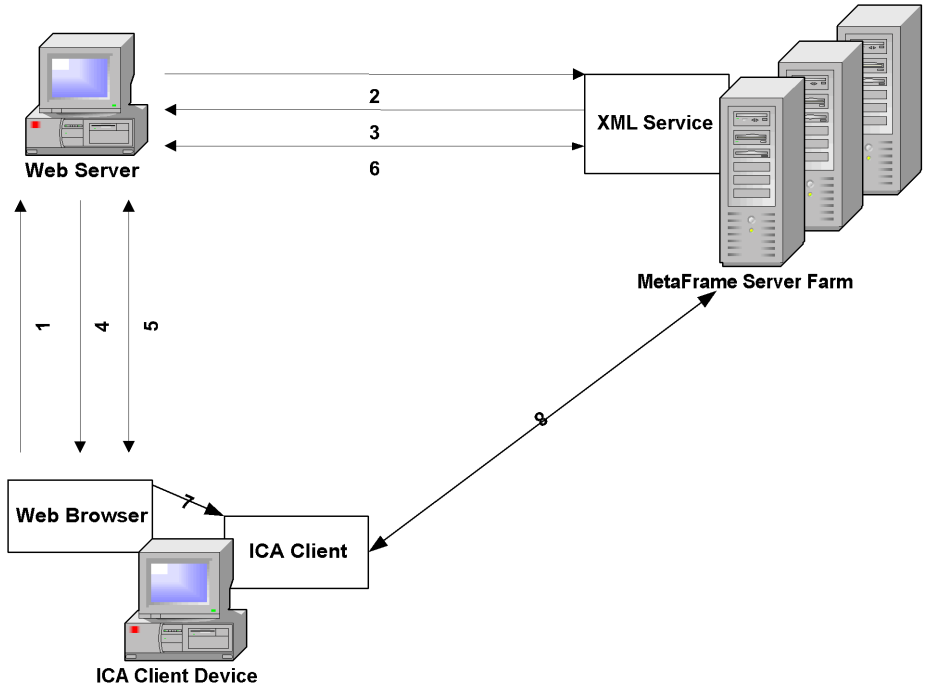
In an ICA Client device, the Web browser and ICA Client work together as a viewer and engine. The Web browser lets users view application sets (created by server-side scripting on the NFuse Classic server) while the ICA Client acts as the engine that launches published applications.

NFuse Classic 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 user visits an NFuse Classic 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-bit 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 83 for more information.

NFuse Classic supports many Web browser/ICA Client combinations. For a complete list of supported browser/client combinations, see “ICA Client Device Requirements” on page 28.

How NFuse Classic Works

This diagram describes a typical interaction between the MetaFrame server farm, an NFuse Classic server, and an ICA Client device.



1. An ICA Client device user utilizes a Web browser to view the NFuse Classic Login page and enters his or her 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 Classic Java objects to forward the information to the Citrix XML Service on a MetaFrame server in the server farm. The designated server acts as a broker between the Web server and the MetaFrame 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 MetaFrame 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 Classic Java objects running on the Web server.
4. The Web server uses the NFuse Classic 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 Classic 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 Classic 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 Citrix XML Service is contacted to locate the least-busy MetaFrame server in the farm.
7. The Web browser receives the ICA file and passes it to the ICA Client device.
8. The ICA Client receives the ICA file and initiates an ICA session with a MetaFrame server according to the ICA file's connection information.

What to Do Next

For information about NFuse Classic system requirements and instructions for installing NFuse Classic and configuring your Web server, see “Deploying NFuse Classic” on page 23.

Deploying NFuse Classic



Overview

This chapter explains how to install NFuse Classic on your Web server and configure the Web server for NFuse Classic. Topics include:

- System requirements
- Installing NFuse Classic on Microsoft IIS
- Installing NFuse Classic on UNIX operating systems
- Configuring your Web server for NFuse Classic
- Troubleshooting NFuse Classic installation
- Uninstalling NFuse Classic

System Requirements

The following section describes MetaFrame server, Web server, and ICA Client device requirements for NFuse Classic.

MetaFrame Server Requirements

To work with NFuse Classic Version 1.7, your MetaFrame servers must meet the following requirements.

Supported MetaFrame Versions

NFuse Classic requires one of the following Citrix platforms:

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

NFuse Classic 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 for Windows Version 1.8 servers must have:

- Citrix MetaFrame 1.8 Service Pack 2 or 3 installed on each server.
- A 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:

- Citrix MetaFrame for UNIX Feature Release 1 installed on each server.
- A Citrix MetaFrame for UNIX Feature Release 1 license installed and activated on each server.
- The Citrix XML Service for UNIX Operating Systems must be running on all MetaFrame for UNIX servers in the farm, on the same TCP port, to support NFuse ticketing.

MetaFrame XP for Windows Version 1.0 servers have no additional software requirements. Service Pack 1/Feature Release 1 and Service Pack 2/Feature Release 2 for MetaFrame XP are supported, but not required. Note, however, that without the Feature Releases some new features will not be available.

For example, 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 Operating Systems. To use DNS addresses with NFuse Classic, 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. Similarly, to use the Enhanced Content Publishing feature with NFuse Classic, you must have Service Pack 2 and a Feature Release 2 license installed on all MetaFrame XP servers in the server farm.

MetaFrame and ICA Client Version Requirements for NFuse Classic Features

The following table summarizes the MetaFrame and ICA Client versions that are required for key NFuse Classic features (note that “FR” denotes “Feature Release”).

NFuse Classic Feature	MetaFrame Requirements	ICA Client Requirements
Ticketing	MetaFrame 1.8 FR1 MetaFrame XP 1.0 MetaFrame for UNIX 1.1 FR1	6.0 or later
NDS authentication	MetaFrame XP FR1	6.20 or later
DNS addressing	MetaFrame XP FR1 MetaFrame for UNIX 1.1 FR1	6.20 or later
Smart card support	MetaFrame XP FR2	6.30 or later
Desktop Credential Pass Through	MetaFrame XP FR2	N/A
Enhanced Content Publishing	MetaFrame XP FR2	6.20 or later
File Type Association for arbitrary documents	MetaFrame XP FR2	6.30 or later
Server-side firewall support	MetaFrame 1.8 FR1 MetaFrame XP 1.0 MetaFrame for UNIX 1.1	N/A
Client-side firewall support	N/A	6.0 or later for SOCKS 6.30 or later for Secure Proxy
Load balancing	MetaFrame 1.8 FR1 MetaFrame XP 1.0 MetaFrame for UNIX 1.1	N/A
End-user change password	MetaFrame XP FR2 Not available on MetaFrame for UNIX	N/A

NFuse Classic Feature	MetaFrame Requirements	ICA Client Requirements
Auto-download ICA Win32 Web Client	N/A	Provided by NFuse Classic
Pass through authentication (single sign-on)	N/A	Full PN ICA Win32 / PN Agent 6.20 or later
Embedded clients	N/A	Provided by NFuse Classic
Citrix Secure Gateway support	MetaFrame 1.8 FR1 MetaFrame XP 1.0 MetaFrame for UNIX 1.1 FR1	6.20.986 or later

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 MetaFrame servers are running MetaFrame 1.8 for Windows, 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*.

Note If you are using NFuse 1.6 or later in a MetaFrame 1.8 for Windows environment, you must change the **AddressResolutionType** from **ipv4-port** to **ipv4**.

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

Backward Compatibility

Server farms composed of MetaFrame XP 1.0, MetaFrame 1.8, or MetaFrame for UNIX Operating Systems servers are backward compatible with:

- NFuse Version 1.5
- NFuse Version 1.51
- NFuse Version 1.6
- NFuse Version 1.61

Web Server Requirements

On Windows Platforms

You can use NFuse Classic on the following Windows platforms and Web servers:

- Internet Information Server 4.0 on Windows NT 4.0
- Internet Information Server 5.0 on Windows 2000 Server family

The NFuse Classic Admin tool is not available on the Windows NT 4.0 platform. If you are using this platform, use the NFuse.conf file to configure NFuse Classic—see “Configuring NFuse Classic Using NFuse.conf” on page 91 for more information.

Important Windows NT 4.0 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 Classic requires this JVM for execution of its Web Server Extension software.

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

On UNIX Platforms

You can use NFuse Classic 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	Tomcat 3.2.4	Sun 1.3.1
	Redhat 7.1	Tomcat 3.2.4	Sun 1.3.1
	Solaris 7	Tomcat 3.2.4	Sun 1.3.1
	Solaris 8	Tomcat 3.2.4	Sun 1.3.1
iPlanet 4.1	Solaris 7	iPlanet 4.1	Sun 1.2.x
	Solaris 8	iPlanet 4.1	Sun 1.2.x
Tomcat 3.2.2	Redhat 6.2	Tomcat 3.2.2	Sun 1.3.1

Web Server	Operating System	Servlet Engine	JDK
IBM HTTP 1.3.12.2	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
	Redhat 6.2	WebSphere 3.5.2	IBM 1.2.2
	Redhat 7.1	WebSphere 3.5.2	IBM 1.2.2
	Solaris 7	WebSphere 3.5.2	IBM 1.2.2
	Solaris 8	WebSphere 3.5.2	IBM 1.2.2

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

In addition to NFuse Classic, you should have a copy of the ICA Clients on your Web server for Web-based installation of the ICA Clients. See the next section for information about supported ICA Client versions and “Copying ICA Client Installation Files to your Web Server” on page 110 for information about copying the ICA Clients to the NFuse Classic server.

ICA Client Device Requirements

To operate with NFuse Classic, your ICA Client devices must have a supported ICA Client and Web browser. With the exception of the ICA DOS Client, all ICA Clients that ship on the Components CD-ROM are compliant with NFuse Classic. The Components CD-ROM is available in your MetaFrame XP Feature Release 2 media or ICA Clients are also available for free download from the Citrix Web site.

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

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 5 and above Netscape Communicator 4.7x and above Netscape Navigator 6.21 and above
Macintosh	6.0.66 and above	Internet Explorer 5 and above Netscape Communicator 4.7x and above Netscape Navigator 6.21 and above
UNIX for Solaris/ SPARC	6.0.915 and above	Netscape Communicator 4.7x and above
Redhat Linux	6.3 and above	Netscape Communicator 4.7x and above Netscape Navigator 6.x and above

Citrix recommends that you deploy the latest ICA Clients to your users, to ensure that they can take advantage of the latest features. 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.

Installing NFuse Classic

This section explains how to install NFuse Classic on your Web server. An overview of NFuse Classic installation is provided, together with instructions about how to install NFuse Classic on different Web servers.

Installation Overview

You can install NFuse Classic Version 1.7 as part of Feature Release 2 / Service Pack 2 for MetaFrame XP installation or separately from MetaFrame XP. These methods are explained in more detail below.

Installing NFuse Classic During MetaFrame XP Installation

MetaFrame XP Setup provides the option to install NFuse Classic during MetaFrame installation. If you choose this option, NFuse Classic is installed on the MetaFrame server and the NFuse Classic Web pages are placed in the Web server's document root directory on the MetaFrame server. This NFuse Classic Web site is fully functional and can be used immediately, without additional configuration.

If, during installation, you choose to change the default Web page, the default Web page for your MetaFrame server is the NFuse Classic Login page.

Note To install NFuse Classic during MetaFrame installation, Microsoft Internet Information Server (IIS) is required.

Installing NFuse Classic Separately from MetaFrame XP

You can install NFuse Classic separately from MetaFrame XP using the Components CD-ROM, or by downloading NFuse Classic 1.7 from the Citrix Web site. For details about the information you are prompted for during the installation of NFuse Classic, see "Required Information" on page 33.

Installation programs for the following Web servers are available:

- Microsoft Internet Information Server (IIS)
- iPlanet, Tomcat, and WebSphere for UNIX platforms

For more information about how to install NFuse Classic, see "Installing NFuse Classic on Microsoft IIS" on page 35 and "Installing NFuse Classic on UNIX Platforms" on page 36.

Upgrading an Existing Installation

You can upgrade to NFuse Classic 1.7 either by installing Feature Release 2 / Service Pack 2 for MetaFrame XP, or by installing NFuse Classic 1.7 from CD-ROM or Web download files.

Upgrading During MetaFrame XP Installation

Feature Release 2 for MetaFrame XP includes NFuse Classic Version 1.7. If you previously installed NFuse Classic during MetaFrame XP installation, installing Feature Release 2 / Service Pack 2 for MetaFrame XP automatically upgrades NFuse Classic to Version 1.7. To install and use NFuse Classic 1.7, you must install MetaFrame XP Feature Release 2 / Service Pack 2 after MetaFrame XP installation is completed.

The NFuse.conf, NFuseErrorsResource.properties, and NFuse.properties files are backed up in <drive>:\Program Files\Citrix\NFuse\BackedUpBy17. Settings in the NFuse.properties file are migrated to the NFuse.conf file—this means that your existing NFuse settings are automatically migrated to NFuse Classic 1.7.

Upgrading Using the Components CD-ROM or Web Download

You can upgrade to NFuse Classic 1.7 using the Components CD-ROM or the NFuse Classic 1.7 files downloaded from the Citrix Web site.

If you are upgrading from NFuse 1.51 (or higher version) to NFuse Classic 1.7, settings in the NFuse.properties file are migrated to the NFuse.conf file—this means that your existing NFuse Classic settings are automatically migrated to NFuse Classic 1.7.

The installer detects the earlier version of NFuse Classic and backs up the NFuse.conf, NFuse.properties, and NFuseErrorsResource.properties files in a backup directory. You are prompted for the location of this backup directory during the installation process; for example, on IIS, this might be: C:\Program Files\Citrix\NFuse\BackedUpBy17. The NFuse Classic Java objects (.jar files), scripts, and ICA files are not backed up and remain in the same location.

After you upgrade to NFuse Classic 1.7, your previous NFuse Classic site continues to work as normal.

Note To upgrade from NFuse 1.5 (or a lower version) to NFuse Classic 1.7, you must first remove the old version of NFuse before installing NFuse Classic 1.7. For information, see the appropriate *Administrator's Guide* for the version of NFuse you want to uninstall. To apply any customizations from your old site to the new site, edit the new NFuse.conf file to include your custom settings. Note, however, that not all of your original NFuse.conf settings may apply in NFuse Classic 1.7. See the table listing NFuse.conf parameters on page 92 for more information.

Citrix Enterprise Services for NFuse Considerations

If you want to upgrade a server that is currently installed with NFuse 1.61 and Enterprise Services for NFuse 1.0, to NFuse Classic 1.7 only (in other words, you want to upgrade to NFuse Classic 1.7 without Enterprise Services for NFuse) you must:

1. Remove Enterprise Services for NFuse 1.0
2. Install NFuse Classic 1.7 (upgrade NFuse 1.61 to NFuse Classic 1.7)

For more information about removing Enterprise Services for NFuse, and about installing NFuse Classic with Enterprise Services for NFuse, see the *Citrix Enterprise Services for NFuse Administrator's Guide*.

What Is Installed Where?

When you install NFuse Classic, files are installed in two main locations: the software directory and the Web server's document root:

- **The software directory.** For example, on Windows this is typically: C:\Program Files\Citrix\NFuse; on UNIX systems, this may be: /usr/local/tomcat/webapps/Citrix/WEB-INF. NFuse Classic software and configuration components are stored here, including:
 - NFuse.properties file
 - NFuse Classic Java objects (.jar files)
 - NFuse.conf file
 - ICA templates (.ica files)

Note In NFuse Classic Version 1.7, on the Windows platform, the NFuse.conf file is stored in: C:\Program Files\Citrix\NFuse\Conf.

The NFuse Classic files in this location are global. Therefore, if you make changes to NFuse.conf, these settings are applied to all Web pages served by NFuse Classic.

- **The Web server's document root.** This depends upon where you installed your Web server—for example, on Windows this is typically: C:\inetpub\wwwroot\Citrix\NFuse17; on UNIX systems, this may be: /usr/local/tomcat/webapps/Citrix/NFuse17. NFuse Classic presentation and layout components are stored in this location, including scripts (.asp, .jsp, and .htm files).

NFuse Classic files in this location can be tailored to specific Web pages. For example, to run two different NFuse Classic sites on one Web server, you can create two directories under the Web server's document root, each with its own custom scripts.

Enterprise Services for NFuse Files

Files for Enterprise Services for NFuse are also installed in the software directory and Web server's document root when you install NFuse Classic 1.7 separately from MetaFrame XP. For example, on Windows, the NFuseE.jar file is installed in <drive>\Program Files\Citrix\NFuse, and various scripts and images in <webroot>\Citrix\NFuseEnterprise. Note, however, that these files are not used unless you install and activate Enterprise Services for NFuse. For more information about Enterprise Services for NFuse, see the *Citrix Enterprise Services for NFuse Administrator's Guide*.

Security Considerations

Citrix recommends that, as with any Windows-based server, you follow Microsoft standard guidelines for configuring your Windows server. In particular, when you install the server, do not use a FAT (File Allocation Table) file system, as this may allow users other than administrators to run the NFuse Classic Admin tool. If you use a FAT file system, no authentication will occur when the NFuse Classic Admin tool is accessed.

Required Information

If you install NFuse Classic separately from MetaFrame XP using the Components CD-ROM or Web download files, you are prompted for information during the installation that includes:

- **MetaFrame server identity.** 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. You can specify 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 names of one or more servers running the Citrix XML Service for UNIX Operating Systems.

- **ICA Clients.** You are prompted for the Components CD-ROM 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 document 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 NFuse Classic 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/<icaclientplatform>.`
- **TCP/IP port.** 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. For more information about how to do this, see the following section.

Viewing the XML Service Port Assignment

If you install NFuse Classic separately from MetaFrame XP using the Components CD-ROM or Web download files, during the installation you are prompted for the port number on which the Citrix XML Service is running. The XML Service is the communication link between the MetaFrame server farm and the NFuse Classic server. This section explains how to display the port number on which the XML Service is running.

► 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.
 If during MetaFrame XP installation the administrator chose the option to share Internet Information Server's TCP/IP port with NFuse Classic, 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 *MetaFrame for UNIX Operating Systems Administrator's Guide*.

Installing NFuse Classic on Microsoft IIS

Important During the installation of NFuse Classic on Microsoft IIS, the installer stops and restarts your Web server and its associated services. This restart causes a disruption of service to connected users for the duration of the installation.

► **To install NFuse Classic on Microsoft IIS**

1. Log on as an administrator.
2. If you are installing NFuse Classic from the Components CD-ROM, insert the CD-ROM in your Web server's CD drive. The Citrix MetaFrame XP Components dialog is displayed. Choose the **NFuse Classic** option.
If you downloaded NFuse Classic from a download site, copy the file NFuseClassic17-IIS.exe to your Web server. Double-click the file.
3. The Installation wizard guides you through the installation process.

CAUTION If, during the installation, you use the command-line option to write details to a log file, or the registry is set to write to a log file when software is installed, the NFuse Classic Admin tool password appears in the log file in clear text. If you distribute the log file, make sure you remove the password from this file.

Installing NFuse Classic on UNIX Platforms

This section describes how to install NFuse Classic on iPlanet, Tomcat, and WebSphere.

NFuse Classic requires a servlet engine to work on UNIX platforms. The iPlanet and Tomcat Web servers include a built-in servlet engine. However, the Apache Web server requires an additional servlet engine to support NFuse Classic such as Tomcat (note that Tomcat can be used as a standalone Web server or as a servlet engine).

During NFuse Classic installation, you are prompted for locations in which to place the NFuse Classic files. See “File Location Information” on page 37 for information about where to install files.

► To install NFuse Classic on iPlanet, Tomcat, and WebSphere

1. Log on as root at the server on which you want to install NFuse Classic.
2. Copy the `NFuseClassic17-UNIX.tar.gz` file from the Components CD-ROM or from the Citrix download site to an install directory on your Web server.
3. Unzip the `NFuseClassic17-UNIX.tar.gz` file to produce `NFuseClassic17-UNIX.tar`, an archive containing the setup files for NFuse Classic.
4. To extract the archived files from `NFuse17-UNIX.tar` into the install directory, type **`tar xvf NFuseClassic17-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 Classic files in the appropriate directories. See “File Location Information” on page 37 for information about where to place NFuse Classic files.
8. When installation is complete, you may need to configure your Web server, depending upon which Web server you are using:
 - For Tomcat, no further configuration is required. Stop and restart the Web server.
 - For WebSphere, see “Configuring WebSphere Web Server” on page 39 for more information.
 - For iPlanet Web server, see “Configuring iPlanet Web Server” on page 39 for more information.

Note Citrix recommends that you retain the contents of the directory to which the .tar file is extracted in case you later want to uninstall NFuse Classic. See “Uninstalling NFuse Classic” for more information.

File Location Information

During NFuse Classic installation, you are prompted for locations in which to place the NFuse Classic files. The following table lists these files by type. Use this table as a reference when installing NFuse Classic and configuring your Web server.

File Type	Description	Directory
NFuse Classic Java objects: nfuse.jar ctxxml4j.jar jsafeObf.jar sslplus3.1.7.jar NFuseE.jar	Java objects including the base NFuse Class files, IBM XML parser, and SSL/SOCKS provider Classes and cryptographic libraries.	On Tomcat, the installer determines the location of these files. On other platforms, place these files in the classpath.
Configuration files: NFuse.conf NFuse.properties NFuse.dtd ctxSTA.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 installer determines the location of these files.
Web pages	NFuse Classic 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/NFuse....

File Type	Description	Directory
Icon files	The setup program creates an icon cache directory that the NFuse Classic 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>/Citrix/NFuse17/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 Classic Web sites to install ICA Clients on client devices.	<p>The setup program prompts the administrator to supply the Components CD-ROM 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.</p> <p>The NFuse Classic Web pages assume the ICA Client files are stored in this directory structure.</p> <p>If the Components CD-ROM is not available, you can copy the contents of the CD's ICAWEB directory to your Web server after setup completes.</p>

Configuring Your Web Server for NFuse Classic

This section explains how to configure the iPlanet and WebSphere Web Servers for NFuse Classic.

Configuring iPlanet Web Server

The following procedure explains how to configure iPlanet Web Server for NFuse Classic.

► **To configure iPlanet Web Server for NFuse Classic**

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 lines (where `<NFuse folder>` is where NFuse Classic is installed; for example `/usr/netscape/server4/Citrix`):

```
<NFuse folder>/nfuse.jar  
<NFuse folder>/NFuseE.jar  
<NFuse folder>/ctxxml4j.jar  
<NFuse folder>/jsafeObf.jar  
<NFuse folder>/sslplus3.1.7.jar  
<NFuse folder>/conf/
```

5. Restart the Web server.

Configuring WebSphere Web Server

The following procedure explains how to configure WebSphere for NFuse Classic.

► **To configure WebSphere Web Server for NFuse Classic**

1. In the “/opt/WebSphere/AppServer/bin” directory, execute the “startupServer.sh” file.
2. Start another shell and execute the WebSphere Standard Administrative Console. For example:

```
/usr/IBMWebAS/bin/adminclient.sh
```
3. When the Administrative Console opens, click the Wizards icon and then choose **Create a Web Application** from the drop-down list.
4. In the first page of the wizard, enter “Citrix” as the Web Application Name. Keep the other defaults and click **next**.

5. In the next page, expand the Nodes tree and highlight the last branch, Default Servlet Engine, and click **next**.
6. In the next page, enter “/Citrix” for the Web Application Web Path. Keep the other defaults and click **next**.
7. In the next page, enter the Document Root—this path depends on where NFuse Classic is installed—for example: “/usr/IBMWebAS/hosts/default_host/Citrix/web/Citrix/.”
8. Under the Classpath heading, enter the following lines (where <NFuse folder> is where NFuse Classic is installed).

Tip To create more space, click the down arrow on the left.

```
<NFuse folder>/nfuse.jar
<NFuse folder>/NFuseE.jar
<NFuse folder>/ctxxml4j.jar
<NFuse folder>/jsafeObf.jar
<NFuse folder>/sslplus3.1.7.jar
<NFuse folder>/conf
```

9. Click **Finish** to end the wizard.
10. Under the WebSphere Administration Domain tree, expand the branch that is the hostname of your server and highlight **Default Server**.
11. In the right-hand pane, Application Server:DefaultServer, enter the following in the Command line arguments field and click **Apply**:


```
-classpath <WebSphere folder>/hosts/default_host/Citrix/
servlets/ctxxml4j.jar:<WebSphere folder>/hosts/default_host/
Citrix/servlets/sslplus3.1.7.jar:<WebSphere folder>/hosts/
default_host/Citrix/servlets/jsafe-Obf.jar
```
12. Start the IBM HTTP service from the appropriate directory (for example: /opt/IBMHTTP/bin) using the command:


```
./apachectl
```
13. Open the WebSphere Standard Administrative Console; for example:


```
./adminclient.sh
```
14. Highlight the **Default Server** (if it is not already highlighted) and click the **stop** button. Wait until you see a dialog box that says: “Command ‘Default Servcer.stop’ completed Successfully”. Close this dialog box.
15. Click the **start** button. The Web service restarts. By default, WebSphere listens on port 80.

Note Restarting WebSphere can take several minutes. A dialog box appears when the installation is completed.

What to Do Next

After you install NFuse Classic and configure your Web server (if necessary), you are ready to make NFuse Classic available to your users.

However, you may need to configure NFuse Classic depending upon what other components are in your MetaFrame installation, or you may want to customize or extend NFuse Classic's capabilities.

- For information about how to configure NFuse Classic for Citrix Secure Gateway using the Admin tool, see “Configuring Citrix Secure Gateway Support” on page 74.
- For information about how to configure NFuse for Enterprise Services for NFuse Classic using the Admin tool, see “Configuring Communication With Enterprise Services for NFuse” on page 89 and the *Enterprise Services for NFuse Administrator's Guide*.
- For information about how to configure NFuse Classic using the Admin tool or NFuse.conf file, see “Configuring NFuse Classic Using the Administration Tool” on page 47 or “Configuring NFuse Classic Using NFuse.conf” on page 91.
- For information about security considerations, see “Configuring NFuse Classic Security” on page 117.
- To extend and customize NFuse Classic functionality, see the *Customizing NFuse Classic* guide.

After you have finished configuring NFuse Classic, inform your users of the URL for the NFuse Classic Login page—for more information, see “Making NFuse Classic Available to Users” on page 107.

Troubleshooting NFuse Classic Installation

This section explains how to use the **Repair** option that is available on the Windows platform to troubleshoot NFuse Classic installation. Also explained is what to do if the **Repair** option is unavailable or does not fix the problem.

The **Repair** option is available only if you installed NFuse Classic 1.7 separately from MetaFrame XP, using the Components CD-ROM or Web download files. If you installed NFuse Classic as part of MetaFrame XP, see the *MetaFrame Administrator's Guide* for troubleshooting information.

Using the Repair Option

If you experience problems with your NFuse Classic 1.7 installation, try using the **Repair** option to fix the problem. The **Repair** option replaces the NFuse Classic Java objects (.jar files). It does not replace the scripts (.asp and .htm files) or the NFuse.conf file.

► **To run the Repair option**

1. Double-click the NFuseClassic17-IIS.exe file. The **Citrix NFuse Classic 1.7 Setup** dialog box is displayed.
2. Choose **Repair** and click **Next**.
3. Follow the instructions on screen.

Note If the **Repair** option does not fix the problem, or this option is unavailable (for example, on UNIX platforms), try uninstalling and then reinstalling NFuse Classic. For information, see “Uninstalling NFuse Classic” on page 43. You must reapply any changes you made in the NFuse.conf file after reinstalling NFuse Classic.

Uninstalling NFuse Classic

If you installed NFuse Classic 1.7 separately from MetaFrame XP using the Components CD-ROM or Web download files, you can uninstall it:

- On Windows, using the **Add/Remove Programs** option available from **Start>Settings>Control Panel**
- On UNIX platforms, using the **Remove** option

If you installed NFuse Classic 1.7 as part of MetaFrame XP, to uninstall NFuse Classic you must uninstall Feature Release 2 / Service Pack 2 for MetaFrame XP. When you remove Feature Release 2 / Service Pack 2 for MetaFrame XP, your previous NFuse Classic version is automatically restored.

When you uninstall NFuse Classic 1.7, all NFuse Classic 1.7 files are removed, including the ICAWEB directory and the NFuse Classic 1.7 backup files. Therefore, if you want to keep any NFuse Classic 1.7 files, copy these to another location before you uninstall NFuse Classic.

Important During the uninstallation of NFuse Classic on Microsoft IIS, the installer stops and restarts your Web server and its associated services. This restart causes a disruption of service to connected users for the duration of the installation.

Uninstalling NFuse Classic on Microsoft IIS

- **To uninstall NFuse Classic on Microsoft IIS**
 1. Use the **Add/Remove Programs** option available from **Start>Settings>Control Panel**.
 2. Follow the instructions on-screen.

Uninstalling NFuse Classic on iPlanet, Tomcat, and WebSphere

On UNIX platforms, use the **Remove** option to uninstall NFuse Classic. You must run this command from within the same directory as the original install, because it relies upon a file in this directory that lists files the Setup program originally installed.

For example, if you extracted the NFuseClassic17-UNIX.tar into the directory: /usr/local/NFuseClassic17, make sure you uninstall from the /usr/local/NFuseClassic17 directory.

► To uninstall NFuse Classic on iPlanet, Tomcat, and WebSphere

1. Log on as root at the server from which you want to remove NFuse Classic.
2. Change to the directory where you originally installed NFuse Classic 1.7.
3. Stop the Web server.
4. Type **./setupNFuse**.
5. Select the **Remove** option.
6. Confirm you want to remove NFuse Classic.

Configuring NFuse Classic



Overview

This chapter explains how to configure and customize NFuse Classic using the Admin tool (the graphical user interface) and the NFuse configuration file. Topics include:

- Deciding which configuration method is best to use
- Configuring NFuse Classic using the Admin tool
- Configuring NFuse Classic using the NFuse configuration file
- Making NFuse Classic available to users

Deciding Which Configuration Method to Use

This section helps you to determine which method of configuring NFuse Classic is best for your needs.

You can configure and customize NFuse Classic using the following methods:

Admin tool. This Web-based graphical user interface allows you to perform day to day administration tasks quickly and easily. For example, you can use the Admin tool to specify the settings that users can adjust on the Settings page, or to configure user authentication to NFuse Classic. After you've made changes using the Admin tool, you save and apply them so your configuration takes effect. The Admin tool is available only on Windows/IIS machines, and requires Internet Explorer version 5.0 or later. For information about how to configure NFuse Classic using the Admin tool, see "Configuring NFuse Classic Using the Administration Tool" on page 47 and the Admin tool online help.

NFuse Classic configuration file. The NFuse.conf file allows you to change many of NFuse Classic's properties, and is available on both Windows and UNIX platforms. You can use this file to perform day to day administration tasks and customize many more settings. You simply edit the values in the NFuse.conf file and then stop and restart your Web server to apply the changes. For information about how to configure NFuse Classic using the NFuse.conf file, see "Configuring NFuse Classic Using NFuse.conf" on page 91.

Web server scripts, Citrix substitution tags, and Java servlets. You can use NFuse Classic's application programming interface (API) to extensively customize your NFuse Classic site. You can use Active Server Pages or JavaServer Pages to write Web server scripts that manipulate the NFuse Classic Java objects. Alternatively, you can use the simplified Citrix substitution tags to access the NFuse Classic Java objects, or you can write your own Java servlets using the NFuse Classic Java objects. For more information, see the *Customizing NFuse Classic Guide*.

Configuring NFuse Classic Using the Administration Tool

NFuse Classic 1.7 includes a Web-based graphical user interface—the Admin tool—that you can use to administer and configure NFuse Classic. The Admin tool allows you to manipulate many of the settings in the NFuse.conf file quickly and easily.

The Admin tool is available only on Windows/IIS machines, and requires Internet Explorer Version 5.0 or later. The Admin tool is not available on the Windows NT 4.0 platform. If you are using Windows NT 4.0, or you are running NFuse Classic on a UNIX platform, use the NFuse.conf file to configure NFuse Classic. For more information, see “Configuring NFuse Classic Using NFuse.conf” on page 91.

Note that you cannot use the Admin tool through an HTTP proxy server or firewall.

Accessing the Admin Tool

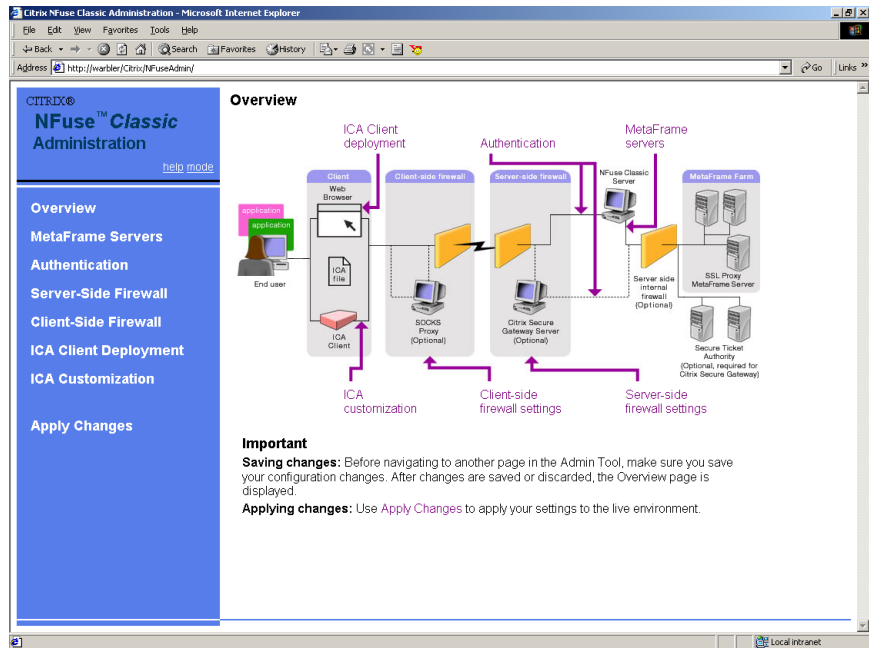
To use the NFuse Classic Admin tool, you must be an administrator on the local NFuse server—in other words, you must belong to the administrator’s group.

When you access the Admin tool, IIS automatically authenticates your credentials using a feature of Internet Explorer and IIS. If you did not access the Windows desktop using a valid administrator account, you are prompted for valid credentials.

► To access the NFuse Classic Admin tool

Type **http://servername/Citrix/NFuseAdmin** in your Web browser, where *servername* is the name of the machine on which NFuse Classic is installed.

When you log on, an **Overview** page similar to the following appears:



The **Overview** page illustrates a typical NFuse Classic deployment, with many of its possible components. The hyperlinks around the graphic provide links to the appropriate configuration pages associated with each component. To navigate the Admin Tool, use these links or the links on the panel on the left side of the page.

Saving, Applying, and Discarding Changes

After you make changes using the Admin tool, click **Save** to save your settings. Click **Discard Changes** to discard any changes made since your last save. When you save or discard changes, the **Overview** page is displayed.

To apply your changes to the live environment, click the **Apply Changes** button in the **Apply changes** page. This reloads the configuration so your settings take effect. After applying changes, the **Overview** page is displayed.

Note Before navigating to another page in the Admin Tool, click **Save** to save any changes you made. If you do not save, your changes are discarded.

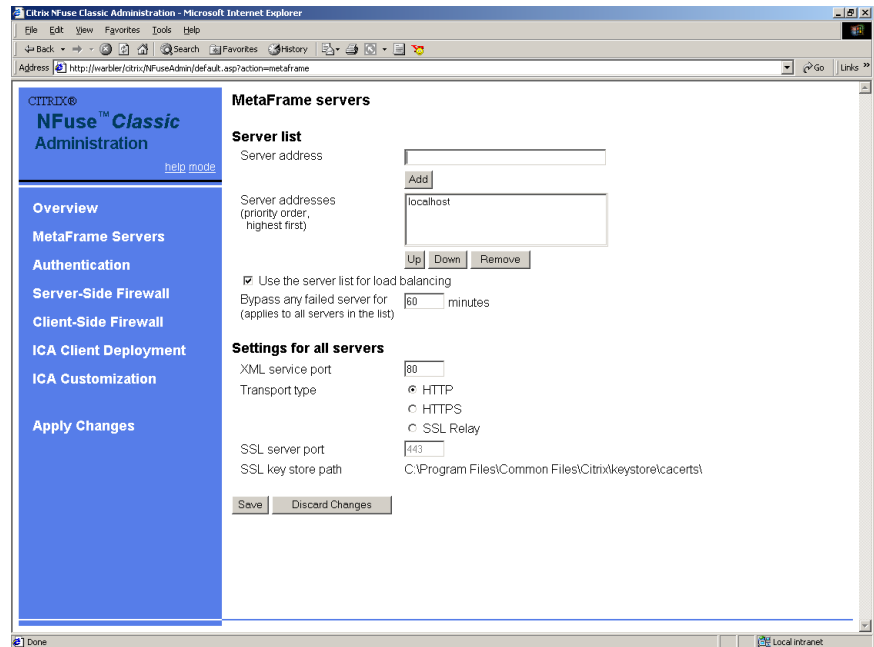
Getting Online Help

You can display context-sensitive online help for the NFuse Classic Admin tool using the **Help** link that is available in the left-hand pane. The help is displayed in a separate browser window.

Configuring Communication With MetaFrame

You can use the **MetaFrame servers** page to specify the names of one or more MetaFrame servers running the Citrix XML Service. The Citrix XML Service is a MetaFrame component that acts as the contact point between the server farm and the NFuse Classic server.

By default, the server name entered during NFuse Classic installation is displayed in the **Server addresses** list.



► To add a server to the list

1. Display the **MetaFrame servers** page.
2. Type the name of the server in the **Server address** field. You can specify a Windows NT server name, IP address, or DNS name.

Note If you are using a secure connection from the Web server to the MetaFrame server (in other words, you set the **Transport type** to **SSL Relay** or **HTTPS**), ensure the server name you specify matches the name on the MetaFrame server's certificate.

3. Click **Add**. The server name is added to the bottom of **Server addresses** list.

4. To specify multiple server names, repeat these steps. To place the servers in the appropriate order, highlight a server name in the **Server addresses** list and use the **Up** and **Down** buttons to place the servers in the appropriate order. The order you specify is important for fault tolerance; see “Configuring Fault Tolerance” for more information.

Note To communicate with an Enterprise Services for NFuse server, rather than with MetaFrame servers running the Citrix XML Service, see “Configuring Communication With Enterprise Services for NFuse” on page 89.

Configuring Fault Tolerance

NFuse Classic provides fault tolerance among servers running the Citrix XML Service. If an error occurs while communicating with a server, the failed server is bypassed for a specified time, and communication continues with the remaining servers in the **Server addresses** list.

By default, a failed server is bypassed for 60 minutes, but you can change this using the **MetaFrame servers** page.

► To configure fault tolerance

1. Display the **MetaFrame servers** page.
2. In the **Server addresses** list, place the servers in order of priority. Highlight a server name in the list and use the **Up** and **Down** buttons to place the servers in the appropriate order.
3. To change the length of time a failed server is bypassed, enter the number of minutes in **Bypass any failed server for**.

Note If a MetaFrame server running the XML Service fails, NFuse Classic will not attempt to communicate with the failed server until the time specified in **Bypass any failed server for** has elapsed. If all servers in the list fail to respond, NFuse Classic will retry the servers every 10 seconds.

Enabling Load Balancing Between Servers

You can enable load balancing between servers running the Citrix XML Service. Enabling load balancing allows you to evenly distribute connections among these servers so that no one server becomes overloaded. By default, load balancing is enabled.

If an error occurs while communicating with a server, all further communication is load balanced between the remaining servers in the list. The failed server is bypassed for a specific time period (by default, 60 minutes) but you can change this using the **Bypass any failed server for** field. See “Configuring Fault Tolerance” on page 50 for more information.

► To enable load balancing

1. Display the **MetaFrame servers** page.
2. In the **Server addresses** list, add the servers that will be load balancing. For information about how to add servers, see “Configuring Communication With MetaFrame” on page 49. The order you specify is important for fault tolerance but not for load balancing.
3. Select the **Use the server list for load balancing** check box.

Specifying the TCP/IP Port for XML Communication

You can specify the TCP/IP port used by the Citrix XML Service on the MetaFrame servers specified in the **Server addresses** list. By default, this is the value of the port number entered during NFuse Classic installation. This port number must match the port number used by the Citrix XML Service.

All MetaFrame servers in the farm must have the Citrix XML Service configured on this port.

► To specify the TCP/IP port

1. Display the **MetaFrame servers** page.
2. Enter the port number in the **XML service port** field.

Specifying the Transport Protocol

You can specify the protocol used to transport NFuse Classic data between the Web server and MetaFrame server. You can choose:

- **HTTP.** Select this to send data over a standard HTTP connection. Use this option if you made other provisions for the security of this link.
- **HTTPS.** Select this to send data over a secure HTTP connection using SSL (Secure Sockets Layer) or TLS (Transport Layer Security). You must ensure that the Citrix XML Service is set to share its port with IIS and that IIS is configured to support HTTPS.
- **SSL Relay.** Select this to send data over a secure connection that uses the Citrix SSL Relay running on the MetaFrame server to perform host authentication and data encryption.

Tip For more information about securing communication using Citrix SSL Relay and HTTPS, see “Configuring NFuse Classic Security” on page 117.

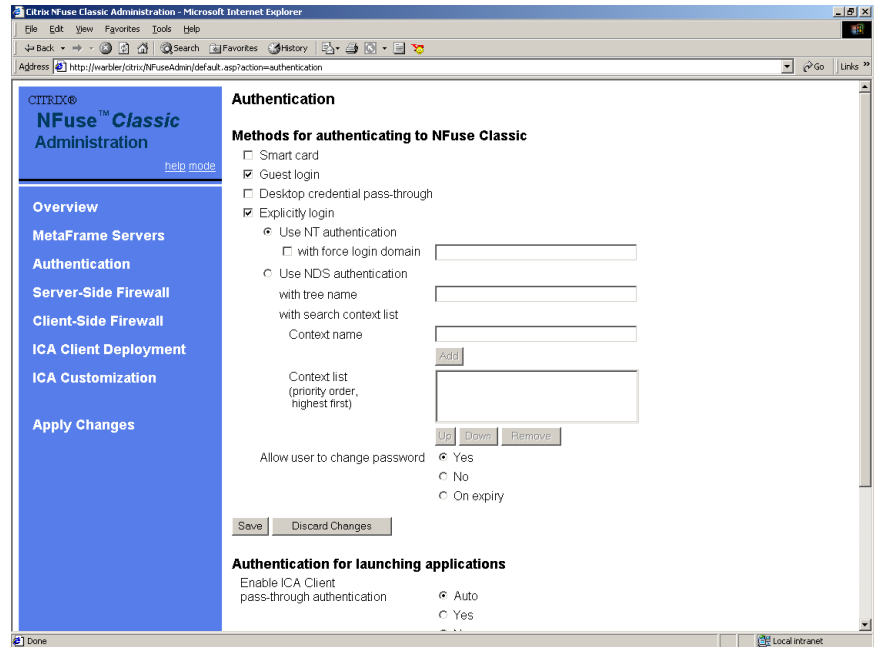
► To specify the transport protocol

1. Display the **MetaFrame servers** page.
2. Select **HTTP**, **HTTPS**, or **SSL Relay**.
3. If you are using **SSL Relay**, specify the TCP port of the SSL Relay in the **SSL server port** field (the default port is 443), and the directory containing the certificate authority root certificates in the **SSL key store path** field. NFuse Classic uses root certificates when authenticating a Citrix SSL Relay server. Ensure all the servers running Citrix SSL Relay are configured to listen on the same port number.

Note If you are using **SSL Relay** or **HTTPS**, ensure the server names you specify match the name on the MetaFrame server's certificate.

Configuring Authentication

You can use the **Authentication** page to configure the ways in which users can authenticate to NFuse Classic and, subsequently, to MetaFrame.



Methods of Authentication

Authentication to NFuse Classic takes place when a user accesses NFuse Classic, using the Login dialog or by another authentication method. If authentication is successful, NFuse Classic returns the user's application set. You can configure the following authentication methods:

- **Explicit**—Users are required to log on to NFuse Classic by supplying a username and password. Microsoft domain-based authentication and Novell Directory Service (NDS) authentication are available.
- **Guest**—Guest users can access NFuse Classic without supplying a username and password and launch applications published for anonymous use on the MetaFrame server.
- **Desktop Credential Pass-Through**—Users can authenticate to NFuse Classic using the credentials they provided when they logged on to their Windows desktop. Users do not need to re-enter their credentials at the NFuse Classic Login page and their application set is automatically displayed.

- **Smart card**—Users can authenticate to NFuse Classic by inserting a smart card into a smart-card reader attached to the client device. The user is prompted for a PIN.

You can also configure how users authenticate to MetaFrame. Authentication to MetaFrame takes place when users click a hyperlink in their application set to launch an application. If authentication is successful, an ICA session is initiated in which the application runs. You can configure:

- **Pass-through authentication.** This is a feature of the ICA Win32 Client that captures users' credentials and passes them to the MetaFrame server for authentication. You can use Desktop Credential Pass-Through and pass-through authentication together to eliminate prompts for user credentials—in other words, to provide users with *single sign-on*.
- **Smart card authentication.** You can configure whether smart cards can be used to authenticate to the MetaFrame server. You can also use this feature in combination with pass-through authentication to minimize the number of prompts for the user's PIN.

Note The type of authentication you specify in NFuse Classic 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 the *ICA Win32 Client Administrator's Guide* for more information about editing the Config.xml file.

Authentication Recommendations

Citrix recommends that you grant your users only the authentication methods that they require. Users can choose how to authenticate to NFuse Classic depending upon the methods you permit. For example, if you allow smart card authentication, guest logons and explicit authentication, users can choose how to authenticate from all of these options.

Do not mix authentication methods. In other words, make sure your users log on to their workstations and NFuse consistently—either explicitly (with a username and password) or using smart cards; not a mixture of both methods. For example, if a user logs on to the Windows desktop using a smart card, and then logs on to NFuse explicitly, the credentials supplied by the client may be incorrect—in this case the client may supply the PIN rather than the username and password.

Configuring Explicit Authentication

By default in the Admin tool, users are required to explicitly log on to NFuse Classic. In other words, users must have a user account and supply a username and password to log on.

You can change the explicit authentication settings using the Admin tool. For example, you can configure whether users are allowed to change their logon passwords within an NFuse Classic session.

► To configure explicit authentication to NFuse Classic

1. Display the **Authentication** page.
2. Select **Explicitly login** to force users to supply a username and password to log on to NFuse Classic.
3. Choose the type of authentication that explicit users must use:
 - Select **Use NT authentication** to specify Microsoft domain-based authentication. To force all users to log on to a specific domain, select the **with force login domain** check box and specify a domain.
 - Select **Use NDS authentication** to specify Novell Directory Service (NDS) authentication. Specify an NDS tree in the **with tree name** field and a context name in the **Context name** field and click **Add**. The context name is displayed in the **Context list**. If you specify more than one context name, highlight a context name in the list and click the **Up** and **Down** buttons to place these in the appropriate order. The order you specify determines the order that context names are displayed to users in the user Login dialog.

Note NDS authentication is supported on IIS/ASP only, because this requires native Win32 Novell NetWare Client DLLs to perform the look-up for the context search.

4. Specify whether users can change their logon passwords within an NFuse Classic session using the **Allow user to change password** field.
 - To let users change their password as often as they want in NFuse Classic, select **Yes**. When you enable this option, the change password icon is displayed on users' pages. When users click on this icon, a dialog is displayed in which users can enter a new password.
 - To let users change their logon password only when the password expires, select **On expiry**. When you enable this option, if a user fails to log on to NFuse Classic due to an expired password, the user is redirected to the change password dialog. After changing their password, the user is automatically logged on to NFuse Classic using the new password.

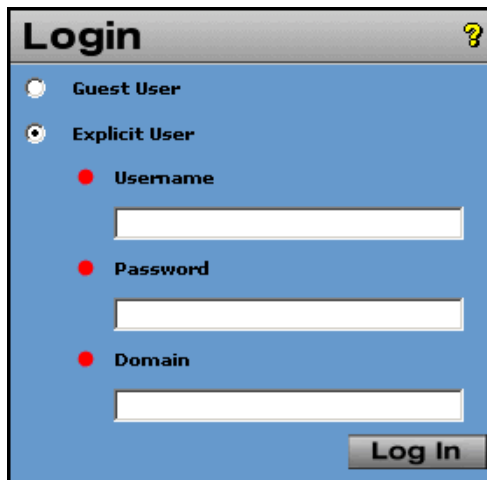
- To prevent users from changing their logon password within NFuse Classic, select **No**.

Note NFuse Classic generates the client name for ICA connections from the username and domain of the user. This name is visible in the Citrix Management Console. However, this name may appear in the console in a shortened form and may contain characters not present in the original username or domain. This ensures unique client names and does not indicate a problem.

For information about configuring ticketing (a feature that provides enhanced authentication security for explicit logons) see “Configuring Ticket Expiry Time” on page 63.

Enabling Guest User Access

You can allow guest users to access NFuse Classic using the Admin tool. When guest user access is enabled, users can log on to NFuse Classic using the Guest User option available in the users' Login page (shown below). Guest users do not have to supply a username or password.



The screenshot shows a web-based login interface. At the top, a grey bar contains the word "Login" in bold black text, followed by a small yellow question mark icon. Below this, the background is blue. There are two radio buttons: the first is labeled "Guest User" and is selected (indicated by a white dot); the second is labeled "Explicit User" and is not selected. Below the "Explicit User" option, there are three red circular icons, each followed by a label and a text input field: "Username", "Password", and "Domain". At the bottom right, there is a grey button with the text "Log In" in bold black text.

Guest users can access applications that the MetaFrame administrator has published for anonymous use. For more information about publishing applications for anonymous use, see your *MetaFrame Administrator's Guide*.

CAUTION Allowing users to log on to NFuse Classic as guests means that these users can obtain Citrix Secure Gateway tickets, despite not being authenticated by NFuse Classic. Because Citrix Secure Gateway relies on NFuse Classic only issuing tickets to authenticated users, this compromises one of the security benefits of using Citrix Secure Gateway in your installation.

► **To enable guest users to access NFuse Classic**

1. Display the **Authentication** page.
2. Select the **Guest login** check box to allow guest users to access NFuse Classic.

Enabling Desktop Credential Pass-Through (Single Sign On)

Using the Admin tool, you can enable Desktop Credential Pass-Through. This is a feature of Internet Explorer and IIS that uses the Windows NT LAN Manager (NTLM) protocol. This feature allows users to authenticate to NFuse Classic using the credentials they provided when they logged into their Windows desktop. Users do not need to re-enter credentials at the NFuse Classic Login page and their NFuse Classic application set is automatically displayed.

You can use Desktop Credential Pass-Through in combination with pass-through authentication, a feature of the ICA Win32 Client. Pass-through authentication captures users' credentials when they log on to their Windows workstations. Later, when an ICA session is initiated, these credentials are passed to the MetaFrame server for authentication. Using Desktop Credential Pass-Through and pass-through authentication together provides users with *single sign-on*.

The following section provides information about Desktop Credential Pass-Through requirements and explains the steps you must perform to enable Desktop Credential Pass-Through and pass-through authentication support. For an example of how to configure single sign-on in NFuse Classic, see "Example 1—Enabling Single Sign On" on page 63.

Desktop Credential Pass-Through Requirements

For the Desktop Credential Pass-Through feature to work, NFuse Classic must be running on IIS and users must be running Internet Explorer Version 5.0 or later, on Windows 2000 or later.

If users are using ICA Clients earlier than Version 6.30 and ICA Encryption (SecureICA) is enabled, pass-through authentication will not work. To use pass-through authentication with ICA Encryption, the latest ICA Clients must be used and your MetaFrame for Windows server must be running MetaFrame XP, Feature Release 2.

CAUTION When a user selects an application, an ICA file is sent to the browser. The ICA file can contain a setting that instructs the client to send the user's workstation credentials to the MetaFrame server. By default the ICA client does not honour this setting. However, there is a risk that if the pass-through authentication feature is enabled on the Win32 ICA Client, an attacker could send the user an ICA file that causes the user's credentials to be misrouted to an unauthorized or counterfeit MetaFrame server. Therefore, do not enable the pass-through authentication feature in a secure installation. Only use this feature in a small, trusted environment.

Step 1—Install the Full ICA Win32 Client

You must install the full ICA Win32 Client on your users' client devices, using an administrator account. The pass-through authentication feature is available only in the full ICA Win32 Client, available on the Components CD-ROM. For security reasons, the downloadable ICA Win32 Clients do not include this feature. This means that you cannot use Web-based ICA Client installation to deploy clients containing this feature to your users.

During installation of the ICA Win32 Client, respond Yes to the prompt "Would you like to enable and automatically use your local user name and password for Citrix sessions from this client?" This enables the pass-through authentication feature; until this feature is enabled, no user of this client device can use pass-through authentication.

Note If you do not enable the pass-through authentication feature during installation of the ICA Win32 Client, you can enable it after installation. In Program Neighborhood, on the **Tools** menu, click **ICA Settings**, and then click the **General** tab and select the **Pass-through Authentication** check box. To do this, you must use an administrator account. For more information about enabling pass-through authentication, see the *ICA Win32 Client Administrator's Guide*.

Step 2—Edit the Appsrv.ini File

You must also edit the Appsrv.ini file, located in users' profiles, to enable pass-through authentication. For example, if a user's profile is stored locally, this file is located in: C:\Documents and Settings\user\Application Data\ICAClient (note that Application Data is a hidden folder).

In the [WFClient] section, add the following entries:

```
EnableSSOnThruICAFile=On
SSOnUserSetting=On
```

Step 3—Enable Desktop Credential Pass-Through Using the Admin Tool

You must configure NFuse Classic to enable Desktop Credential Pass-Through authentication. When you enable this feature, users do not need to enter their credentials again to access NFuse Classic and their application set is automatically displayed.

► **To allow users to authenticate using Desktop Credential Pass-Through**

1. Display the **Authentication** page.
2. Select the **Desktop credential pass-through** check box to allow users to authenticate to NFuse Classic using their Windows desktop logon credentials.

Step 4—Enable Pass-Through Authentication Using the Admin Tool

You can configure NFuse Classic to allow pass-through authentication of the user's credentials to the MetaFrame server. This means that users are not prompted again for their credentials when they launch an application. By combining Desktop Credential Pass-Through with pass-through authentication, you provide users with *single sign-on*.

► **To enable pass-through authentication**

1. Display the **Authentication** page.
2. In the **Authentication for launching applications** section, set **Enable ICA Client pass-through authentication** to allow users to authenticate to MetaFrame using pass-through authentication. Choose from one of the following options:
 - **Auto.** This is the default. If the user authenticated to NFuse Classic using Desktop Credential Pass-Through, NFuse Classic attempts to authenticate to MetaFrame using pass-through authentication, and the ICA Client passes the captured credentials to the MetaFrame server.
 - **Yes.** NFuse Classic always attempts to authenticate to MetaFrame using pass-through authentication. The ICA Client passes the captured credentials to the MetaFrame server.
 - **No.** NFuse Classic never attempts to authenticate to MetaFrame using pass-through authentication.

Enabling Smart Card Authentication

Smart cards are credit-card sized plastic cards with embedded computer chips. Smart cards can contain memory only, memory with security logic, or memory with CPU capabilities. Smart cards can be used to secure communications over a network and to provide authentication between clients and servers.

Users can authenticate to NFuse Classic using smart cards. The user inserts the smart card into a smart-card reader attached to the client device, and then is prompted for a PIN.

You can use the Admin tool to enable smart card authentication to NFuse Classic and to the MetaFrame server. You can also configure pass-through authentication of the user's PIN, so that when a user launches an application, the user is authenticated on the MetaFrame server. This reduces the number of prompts for the user's PIN.

The following section provides information about smart card requirements and explains the steps that you must perform to enable smart card support. For an example of how to configure smart card authentication in NFuse Classic, see "Example 2—Enabling Smart Card Authentication" on page 64.

Smart Card Support Requirements

For smart card authentication to work, NFuse Classic must be running on IIS and users must be running Internet Explorer Version 5.0 or later on Windows 2000 or later. Smart card support is not available on Windows NT 4.0 or UNIX platforms.

SSL must be enabled on the Web server. Because Secure Sockets Layer (SSL) is the mechanism underlying smart card technology, SSL must be used between the browser and Web server. See your Web server documentation for further information.

For more information about client device requirements and MetaFrame server requirements for smart card support, see the *ICA Win32 Client Administrator's Guide* and the *MetaFrame Administrator's Guide*.

Step 1—Install the Full ICA Win32 Client

You must install the full ICA Win32 Client on your users' client devices, using an administrator account. The pass-through authentication feature, necessary for smart card support, is available only in the full ICA Win32 Client on the Components CD-ROM. For security reasons, the downloadable ICA Win32 Clients do not include this feature. This means that you cannot use Web-based ICA Client installation to deploy clients containing this feature to your users.

During installation of the ICA Win32 Client, respond Yes to the prompt “Would you like to enable and automatically use your local user name and password for Citrix sessions from this client?”. This enables the pass-through authentication feature. If this feature is not enabled, no user of this client device can use pass-through authentication.

Note If you do not enable the pass-through authentication feature during installation of the ICA Win32 Client, you can enable it after installation. In Program Neighborhood, on the **Tools** menu, click **ICA Settings**, and then click the **General** tab and select the **Pass-through Authentication** check box. To do this, you must use an administrator account. For more information about enabling pass-through authentication, see the *ICA Win32 Client Administrator's Guide*.

Step 2 (OPTIONAL)—Edit the Appsrv.ini file

If you want to configure pass-through authentication to reduce the number of prompts for the user's PIN, you must edit the Appsrv.ini file, located in users' profiles to enable pass-through authentication. For example, if a user's profile is stored locally, this is located in:

C:\Documents and Settings\user\Application Data\ICAClient
(note that Application Data is a hidden folder).

In the [WFClient] section, add the following entries:

```
EnableSSOnThruICAFile=On  
SSOnUserSetting=On
```

Note Enabling pass-through authentication poses a security risk—see the Caution on page 58 for more information.

Step 3—Enable the Windows Directory Service Mapper

You must ensure the Windows Directory Service Mapper is enabled on your NFuse Classic server.

NFuse authentication uses Windows domain accounts—that is, username and password credentials. However, certificates are stored on smart cards as User Principal Names (UPNs). The Directory Service Mapper maps a UPN to a Windows domain account, using Windows Active Directory.

► To enable the Windows Directory Service Mapper

1. Open the Internet Information Services Snap-in tool within the Microsoft Management Console on the NFuse Classic server.

2. Navigate to the node labelled <machine-name>, where *machine-name* is the name of your NFuse Web server. Right-click and choose **Properties**.
3. From the **Internet Information Services** tab, ensure **WWW Service** is shown in the **Master Properties** section and choose **Edit**.
4. From the **Directory Security** tab, select **Enable the Windows directory service mapper**.
5. Click **OK** to enable the Directory Service Mapper.

Step 4—Enable Smart Card Authentication Using the Admin Tool

You must configure NFuse Classic to enable smart card authentication to NFuse Classic (so that users can access NFuse Classic and display their application set) and to the MetaFrame server (so that users can launch applications in an ICA session using NFuse Classic).

You can also configure NFuse Classic to allow pass-through authentication of the users' PIN, so that the user is not prompted again for their PIN when they launch an application.

► To allow users to authenticate using smart cards

1. Display the **Authentication** page.
2. Select the **Smart card** check box to allow users to authenticate to NFuse Classic using a smart card.
3. In the **Authentication for launching applications** section, set **Use smart card to log in to MetaFrame** to enable smart card authentication to MetaFrame. Choose from one of the following options:
 - **Auto**. This is the default. If the user authenticated to NFuse Classic using a smart card, NFuse Classic attempts to authenticate to MetaFrame using this method.
 - **Yes**. NFuse Classic always attempts to authenticate to MetaFrame using smart card credentials.
 - **No**. NFuse Classic never attempts to authenticate to MetaFrame using smart card credentials.

Note If **Use smart card to log in to MetaFrame** is set to **Yes** but a smart card is not available, a dialog box requesting the users to press CTRL-ALT-DEL appears. If this occurs, you must tell your users to press CTRL and F1 to bypass this dialog box and then enter their username and password to log on to MetaFrame.

4. To configure pass-through authentication of the user's PIN, in the **Authentication for launching applications** section, set **Enable ICA Client pass-through authentication**. You can choose from one of the following options:
 - **Auto**. This is the default. If the users authenticated to NFuse Classic using a smart card, the ICA Client does not pass the captured PIN to the MetaFrame server, and users are prompted for their PIN. This is the most secure method.
 - **Yes**. NFuse Classic always attempts to authenticate to MetaFrame using pass-through authentication. The ICA Client passes the captured PIN to the MetaFrame server and users are not prompted for their PIN. Note that this method is not as secure as prompting for the PIN.
 - **No**. NFuse Classic never attempts to authenticate to MetaFrame using pass-through authentication.

Configuring Ticket Expiry Time

Using the **Authentication** page, you can specify an expiry time for the ticket generated by the MetaFrame server. Ticketing provides enhanced authentication security for explicit logons by eliminating user credentials from the ICA files sent from the Web server to the client devices.

Each NFuse Classic ticket has an expiry time which, by default, is 200 seconds; however, you can configure this. For example, you may want to tune this to your network's performance, because expired tickets cannot successfully authenticate a user to the MetaFrame server farm.

- **To configure the expiry time of tickets**
 1. Display the **Authentication** page.
 2. To change the expiry time of tickets, enter a value in seconds in the **MetaFrame ticket time to live** field. By default, the expiry time is 200 seconds.

Examples

Example 1—Enabling Single Sign On

This example illustrates the steps required to allow users to launch applications with NFuse Classic using only the credentials they provided when they logged into their Windows desktop.

You want to enable single sign on for the user Ken by combining Desktop Credential Pass-Through and pass-through authentication. Ken is using a Windows 2000 client device with locally stored profiles. To enable single sign on for Ken:

1. Use the Components CD-ROM to install the full ICA Win32 Client on Ken's client device. The installation of the client is performed using an administrator account. During installation, respond Yes to the prompt "Would you like to enable and automatically use your local user name and password for Citrix sessions from this client?" This enables the pass-through authentication feature.
2. Edit the Appsrv.ini file located in Ken's profile. This is located in: C:\Documents and Settings\Ken\Application Data\ICAClient. In the [WFClient] section, add the following entries:

```
EnableSSOnThruICAFile=On  
SSOnUserSetting=On
```
3. Use the NFuse Classic Admin tool to configure authentication. In the **Authentication** page:
 - Select **Desktop credential pass-through**. This allows users to authenticate to NFuse Classic using their Windows desktop logon credentials. This means that Ken does not have to re-enter his credentials to log on to NFuse Classic.
 - Set **Enable ICA Client pass-through authentication** to **Auto**. This allows users who authenticated to NFuse Classic using Desktop Credential Pass-Through to automatically authenticate to MetaFrame using pass-through authentication. This means that Ken does not have to re-enter his credentials when he clicks on a hyperlink to launch an application in NFuse Classic.
4. Click **Save** to save the changes and then click the **Apply Changes** button in the **Apply changes** page.

Note The credentials that Ken uses to log on to his Windows desktop must also be valid on the MetaFrame server.

Example 2—Enabling Smart Card Authentication

This example illustrates the steps required to allow a user to log on to NFuse Classic and launch applications using a smart card.

You want to enable smart card authentication for the user Jo. Jo is using a Windows 2000 client device with locally stored profiles. A smart card reader is attached to her client device, and smart card support is configured on the MetaFrame server. Currently, NFuse Classic is configured only to allow explicit authentication using a username and password.

To enable smart card authentication for Jo:

1. Use the Components CD-ROM to install the full ICA Win32 Client on Jo's client device. The installation of the client is performed using an administrator account. During installation, respond Yes to the prompt "Would you like to enable and automatically use your local user name and password for Citrix sessions from this client?" This enables the pass-through authentication feature.
2. Edit the Appsrv.ini file located in Jo's profile. This is located in: C:\Documents and Settings\Jo\Application Data\ICAClient
In the [WFClient] section, add the following entries:
`EnableSSOnThruICAFile=On`
`SSOnUserSetting=On`
3. Ensure that the Windows Directory Service Mapper is enabled. For more information, see "Step 3—Enable the Windows Directory Service Mapper" on page 61.
4. Use the NFuse Classic Admin tool to configure smart card authentication. In the **Authentication** page:
 - Select **Smart card** to allow users to authenticate to NFuse Classic using a smart card device attached to the client device. This means that when Jo chooses Smart Card in the NFuse Classic Login dialog, she only has to enter her PIN to log on to NFuse Classic (assuming she logged on to her Windows desktop using her smart card).
 - Set **Enable ICA Client pass-through authentication** to **Auto**.
 - Set **Use smart card to log in to MetaFrame** to **Auto** so that if the user logged on to NFuse Classic using a smart card, NFuse Classic attempts to authenticate to the MetaFrame server using a smart card. The ICA Client passes the captured smart card credentials to the MetaFrame server. This means that when Jo clicks on a hyperlink to launch an application in NFuse Classic, she has to re-enter her PIN.

Note If you do not want Jo to have to re-enter her PIN when she launches an application in NFuse Classic, set **Enable ICA Client pass-through authentication** to **Yes**. This means that the ICA Client will pass the captured PIN to the MetaFrame server, providing Jo with single sign-on. However, this method is not as secure as setting **Enable ICA Client pass-through authentication** to **Auto**.

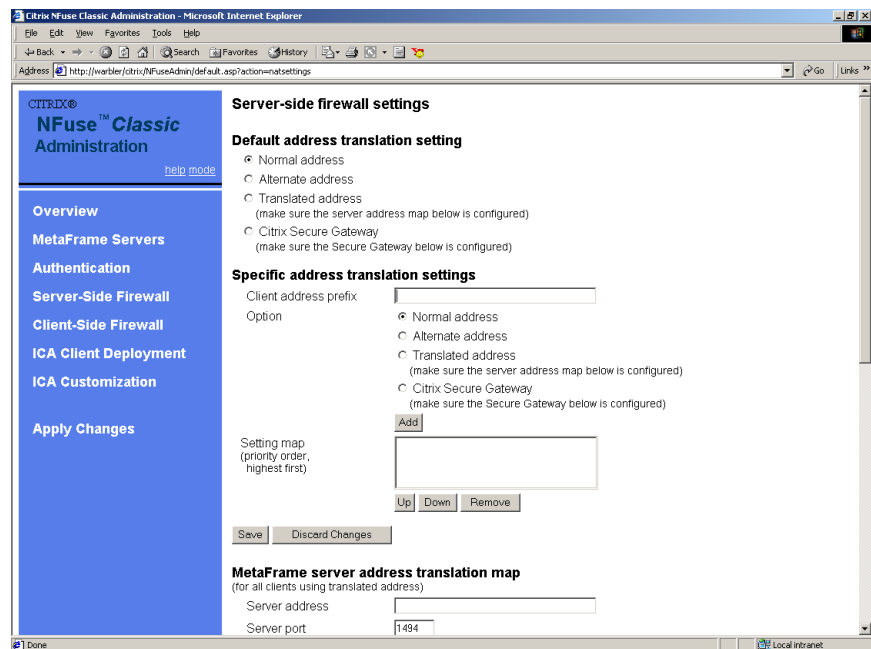
5. Click **Save** to save the changes and then click the **Apply Changes** button in the **Apply changes** page.

Configuring Address Translation

If you are using a firewall in your MetaFrame installation, you can use the **Server-side firewall settings** page to configure NFuse Classic to include the appropriate IP address in .ica files, depending upon how you configured your firewall and your MetaFrame servers.

For example, you can configure NFuse Classic to provide an alternate address, if the MetaFrame server is configured with an alternate address, and the firewall is configured for network address translation (NAT).

This section explains how to configure address translation using the Admin tool, and provides examples of typical scenarios to illustrate this.



About Address Translation

You can configure the following types of addressing within NFuse Classic:

- **Normal addressing.** The IP address given to the client is the actual address of the MetaFrame server. This is the default setting, but you can change this.

- **Network address translation.** Some firewalls use IP address translation to convert private (internal) IP addresses into public (external) IP addresses. If you are using a firewall with network address translation enabled, and you configured your MetaFrame server(s) for this feature, you need to configure NFuse Classic to supply the appropriate IP address, depending upon whether clients connect from inside or outside the firewall. If an external user traverses the firewall to connect to MetaFrame, NFuse Classic provides the external IP address; if a user inside the firewall connects, NFuse Classic provides the internal IP address.
- **Port address translation.** You can define mappings from internal MetaFrame IP addresses to external IP addresses and ports. Using this feature, you can route traffic to internal MetaFrame servers through a single external IP address. For example, you can use this feature to expose only one IP address with several ports. The firewall forwards connections to the appropriate server based on the port number specified by the client.

Specifying the Default Behavior

You can specify what the default behavior is (for example, the type of address translation that NFuse Classic supports) in the **Default address translation setting** section.

For example, if network address translation is enabled at the firewall, you can specify that the default behavior is to use an alternate address. You can also configure exceptions to the default behavior using **Specific address translation settings**.

See “Examples” on page 70 for examples of how to configure default behavior.

► To configure default server-side firewall settings

1. Display the **Server-side firewall settings** page.
2. Under **Default address translation setting**, select one of the following options:
 - **Normal address.** The IP address given to the client is the actual address of the MetaFrame server. This is the default setting.
 - **Alternate address.** The alternate address is given to the client. The MetaFrame server must be configured with an alternate address and the firewall configured for network address translation.
 - **Translated address.** The address given to the client is determined by the address translation mappings set in NFuse Classic. If you select this option, you must define mappings in the **MetaFrame server address translation map**. See “Defining Address Translation Mappings” on page 69 for information.

- **Citrix Secure Gateway.** Configure Citrix Secure Gateway support. If you select this option, you must specify settings in the **Secure Gateway server** section—see “Configuring Citrix Secure Gateway Support” on page 74 for information.

Configuring Specific Address Translation Settings

You can configure address translation settings for specific IP addresses or partial IP addresses (sometimes called *IP address prefixes*). This is useful when you want to configure exceptions to the default behavior.

For example, if network address translation is enabled at the firewall and the default behavior is to use an alternate address, you can specify normal addressing for users on a particular internal subnet.

See “Examples” on page 70 for examples of how to configure exceptions to the default behavior.

Note You can configure mappings for specific IP addresses or partial IP addresses (IP address prefixes) only. If you specify a partial IP address, a simple comparison is performed. For example, if you specify the partial address 10.70. this matches all addresses beginning 10.70., such as 10.70.121.9 and 10.70.4.11. It does not match 10.72.99.2 or 192.10.70.1. Subnet masks and asterisks used as wildcards (such as 10.*.128.12.) are not supported.

► To configure specific address translation settings

1. Display the **Server-side firewall settings** page.
2. In the **Specific address translation settings** section, specify the client IP address or partial IP address prefix in **Client address prefix**.
3. Select one of the following options:
 - **Normal address.** The IP address given to the client is the actual address of the MetaFrame server. This is the default setting.
 - **Alternate address.** The alternate address is given to the client. The MetaFrame server must be configured with an alternate address and the firewall configured for network address translation.
 - **Translated address.** The address given to the client is determined by the address translation mappings set in NFuse Classic. If you select this option, you must define mappings in the **MetaFrame server address translation map**. See “Defining Address Translation Mappings” on page 69 for information.

- **Citrix Secure Gateway.** Configure Citrix Secure Gateway support. If you select this option, you must specify settings in the **Secure Gateway server** section—see “Configuring Citrix Secure Gateway Support” on page 74 for information.
4. Click **Add**. The setting is displayed in the **Setting map** list.
 5. If you configure multiple settings, you can control the order in which these are applied. Highlight the setting and click the **Up** and **Down** buttons to place the settings in order of priority.

Tip To remove a setting, highlight the setting in the **Setting map** list and click **Remove**.

Defining Address Translation Mappings

You can use NFuse Classic to define mappings from internal MetaFrame IP addresses to external IP addresses and ports using the **MetaFrame server address translation map** section. For example, if your MetaFrame server is not configured with an alternate address, you can configure NFuse Classic to provide an alternate address.

See “Examples” on page 70 for an example of how to configure address translation mappings.

1. Display the **Server-side firewall settings** page.
2. Ensure that **Translated address** in **Default address translation setting** or **Specific address translation settings** is selected, as appropriate.
3. In **Server address**, type the normal (internal) IP address or FQDN (Fully Qualified Domain Name) of the MetaFrame server.

Note The value of **AddressResolutionType** in NFuse.conf determines whether the normal MetaFrame server address must be a FQDN or IP address. If AddressResolutionType is set to DNS-port or DNS, all normal addresses must be FQDNs; if AddressResolutionType is set to IPv4-port or IPv4, all normal addresses must be IP addresses.

4. In **Server port**, type the port number of the MetaFrame server. The default port is 1494.
5. In **Translated address**, type the translated (external) IP address or FQDN that clients must use to connect to the MetaFrame server.
6. In **Translated port**, type the port number of the MetaFrame server. The default port is 1494.

7. Click **Add**. The mapping appears in the **Translation map** list.
8. To control the order in which multiple mappings are applied, highlight a mapping and click the **Up** and **Down** buttons to place the mappings in order of priority.

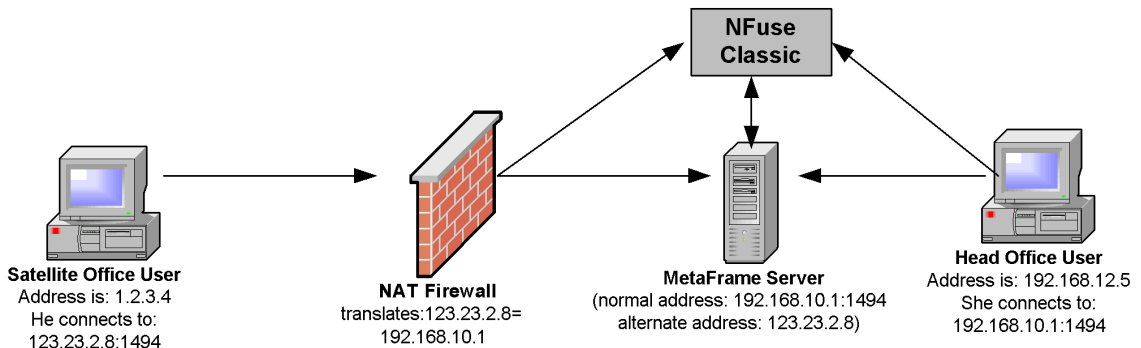
Tip To remove a mapping, highlight the mapping in the **Translation map** list and click **Remove**.

Examples

This section provides examples of typical scenarios to illustrate how to configure address translation using the Admin tool.

Example 1—Configuring Network Address Translation

In this example, network address translation (NAT) is enabled at the firewall. The administrator configures NFuse Classic to include the appropriate address in .ica files for users inside and outside the firewall.



Citrix MetaFrame and NFuse Classic are deployed to provide users with access to applications running on a MetaFrame server in the head office. This server, together with users in the head office, are on the 192.168 subnet. There are also users in a satellite office on the 1.2 subnet, who also require access to these applications. The registered external IP address of the MetaFrame server is 123.23.2.8.

Solution 1—Alternate Addressing Is Configured on the MetaFrame Server

The firewall at the head office uses network address translation to convert external addresses into internal addresses. The MetaFrame server is configured with an alternate address.

Specify that the default behavior is to use an alternate address, and configure exceptions for clients connecting within the firewall, as follows:

1. Display the **Server-side firewall settings** page.
2. Under **Default address translation setting**, select **Alternate address**. This means that the external address of the MetaFrame server is returned by default.
3. Under **Specific address translation settings**, enter 192.168. in the **Client address prefix**.
4. Select **Normal address**.
5. Click **Add**. In the **Setting map** list, **192.168 = Normal** is displayed. This means that for clients connecting on the 192.168 subnet, an internal address is returned.
6. Click **Save** to save the changes.
7. Click **Apply Changes** in the **Apply changes** page.

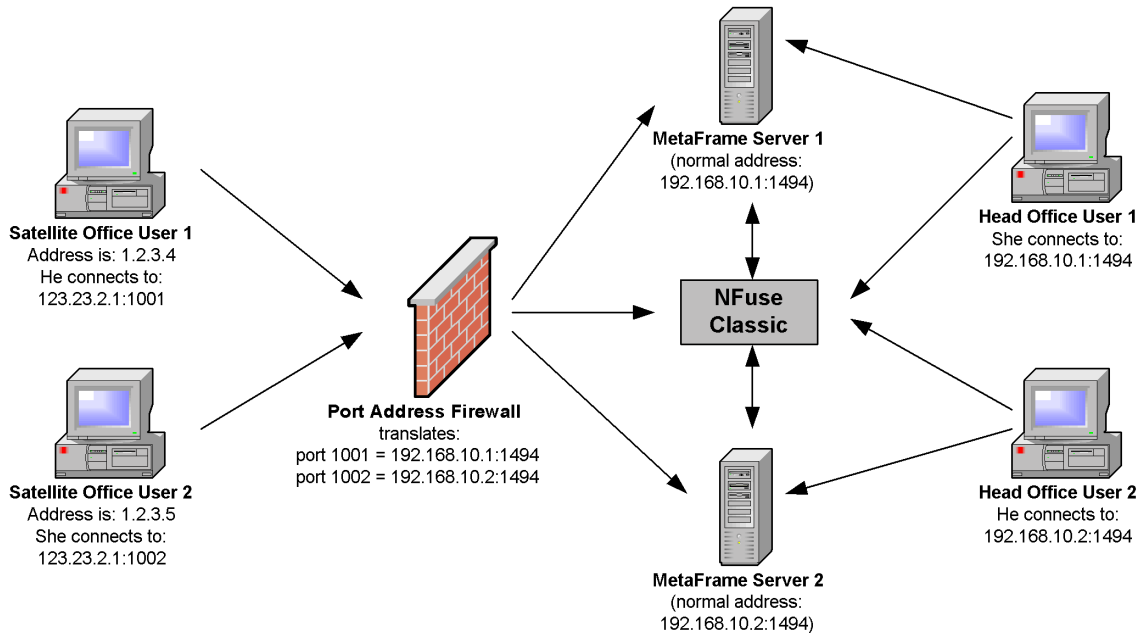
Solution 2—Alternate Addressing Is not Configured on the MetaFrame Server

Alternatively, if the MetaFrame server is not configured with an alternate address, you can configure NFuse Classic to include the appropriate address in the .ica files by defining address translation mappings, as follows:

1. Display the **Server-side firewall settings** page.
2. Select **Translated address** in **Default address translation setting**.
3. Under **Specific address translation settings**, enter 192.168. in the **Client address prefix**.
4. Select **Normal address**.
5. Click the **Add** button. **192.168 = Normal** is displayed in the **Setting map** list. This means that for clients connecting on the 192.168 subnet, an internal address is returned.
6. Under **MetaFrame server address translation map**, type 192.168.10.1:1494 in **Server address**.
7. In **Translated address**, type 123.23.2.8:1494.
8. Click **Add**. In the **Translation map** list, **192.168.10.1:1494 = 123.23.2.8:1494** is displayed. This means that for clients connecting on the 123.23 subnet, NFuse Classic uses the translated address specified.
9. Click **Save** to save the changes.
10. Click **Apply Changes** in the **Apply changes** page.

Example 2—Configuring Port Address Translation

In this example, port address translation is enabled at the firewall. The administrator configures NFuse Classic to include the appropriate address in .Ica files for users inside and outside the firewall.



Citrix MetaFrame and NFuse Classic are deployed to provide users with access to applications running on two MetaFrame servers. The servers and the head office users are on the 192.168 subnet, inside the firewall. The server addresses are 192.168.10.1 and 192.168.10.2. Both servers use the default port 1494. The registered external IP address is 123.23.2.1. However, there are also users in a satellite office on the 1.2 subnet who require access to these applications.

Specify that the default behavior is to use address translation mappings and configure exceptions for clients connecting within the firewall, as follows:

1. Display the **Server-side firewall settings** page.
2. Select **Translated address** in **Default address translation setting**.
3. Under **Specific address translation settings**, enter 192.168. in the **Client address prefix**.
4. Select **Normal address**.

5. Click **Add**. In the **Setting map** list, **192.168 = Normal** is displayed. This means that for clients connecting on the 192.168 subnet, an internal address is returned.
6. Under **MetaFrame server address translation map**, type 192.168.10.1 in **Server address**.
7. In **Translated address**, type **123.23.2.1**
8. In **Translated port**, type **1001**
9. Click **Add**. In the **Translation map** list, **192.168.10.1:1494 = 123.23.2.1:1001** is displayed.
10. Type **192.168.10.2** in **Server address**.
11. In **Translated address**, type **123.23.2.9**
12. In **Translated port**, type **1002**
13. Click **Add**. In the **Translation map** list, **192.168.10.2:1494 = 123.23.2.9:1002** is displayed. This means that for clients connecting on the 1.2 subnet, NFuse Classic uses the translated address specified.
14. Click **Save** to save the changes.
15. Click **Apply Changes** in the **Apply changes** page.

Configuring Citrix Secure Gateway Support

If you are using Citrix Secure Gateway in your MetaFrame installation, you must configure NFuse Classic for Citrix Secure Gateway support. This section explains how to configure Citrix Secure Gateway support using the Admin tool.

Citrix Secure Gateway acts as a secure Internet gateway between SSL/TLS-enabled ICA Clients and MetaFrame XP servers. The Internet portion of ICA traffic between client devices and the Citrix Secure Gateway server is encrypted using SSL/TLS. This means that users can access information remotely without compromising security. Citrix Secure Gateway also simplifies certificate management, because you require a certificate only on the Citrix Secure Gateway server, rather than on every MetaFrame server in the farm.

Citrix Secure Gateway ticketing is the mechanism used to notify Citrix Secure Gateway that a user is authenticated and should be granted access to the farm. Tickets are generated and verified by the Citrix Secure Gateway Secure Ticket Authority server. When a user selects an application in NFuse Classic, NFuse Classic sends the address of the MetaFrame server on which the application resides to the Secure Ticket Authority in return for a ticket. This ticket is later exchanged by the Citrix Secure Gateway for the address of the MetaFrame server. The use of tickets enhances security, because the internal network addresses of MetaFrame servers are hidden.

See “Example” on page 76 for an example of how to configure Citrix Secure Gateway support. For more information about Citrix Secure Gateway, see the *Citrix Secure Gateway Administrator's Guide*.

The screenshot displays the Citrix NFuse Classic Administration web interface within a Microsoft Internet Explorer browser window. The address bar shows the URL: `http://warbler/Citrix/NFuseAdmin/default.asp?action=netsettings`. The interface is divided into a left-hand navigation pane and a main content area.

Left-hand navigation pane:

- CITRIX®
- NFuse™ Classic Administration
- help mode
- Overview
- MetaFrame Servers
- Authentication
- Server-Side Firewall
- Client-Side Firewall
- ICA Client Deployment
- ICA Customization
- Apply Changes

Main content area:

Secure Gateway server
(for all clients using Citrix Secure Gateway)

Server port: 1494
Translated address:
Translated port: 1494
Add

Translation map (priority order, highest first):
Up Down Remove

Save Discard Changes

Secure Ticket Authorities
URL:
Add

Secure Ticket Authority list (priority order, highest first):
Up Down Remove

☒ Use the Secure Ticket Authority list for load balancing

Save Discard Changes

► **To configure NFuse Classic to support Citrix Secure Gateway**

1. Display the **Server-side firewall settings** page.
2. Choose **Citrix Secure Gateway** in **Default address translation setting** or **Specific address translation settings**, depending on whether you want to configure default behavior or specific settings. If you configure a setting in **Specific address translation settings**, click **Add** to display this in the **Setting map** list.
3. In the **Secure Gateway server** section, specify the Fully Qualified Domain Name (FQDN) of the Citrix Secure Gateway server that ICA Clients must use in the **Address (FQDN)** field. This must match what is on the certificate.
4. Specify the port number on the Secure Gateway server that ICA Clients must use in the **Port** field. The default port number is 443.
5. If network address translation is enabled on the firewall between the Secure Gateway server and the MetaFrame server, select the **Use alternate address of MetaFrame server** check box. Only select this if the MetaFrame server is configured for network address translation.
6. In the **URL** field, specify the DNS name or IP address of a Secure Ticket Authority that NFuse Classic can use. Typically, the **URL** field is pre-filled with a template URL and you need to change only the **<server>** part of the template. However, in more customized installations, you may need to edit the entire URL field. The URL must begin with “http://”.
7. Click **Add**. The Secure Ticket Authority is displayed in the **Secure Ticket Authority list**. You can specify up to 256 Secure Ticket Authorities in this list.
8. To place the Secure Ticket Authorities in order of priority, highlight a Secure Ticket Authority and click the **Up** and **Down** buttons.

Tip To remove a Secure Ticket Authority, highlight it in the **Secure Ticket Authority list** and click **Remove**.

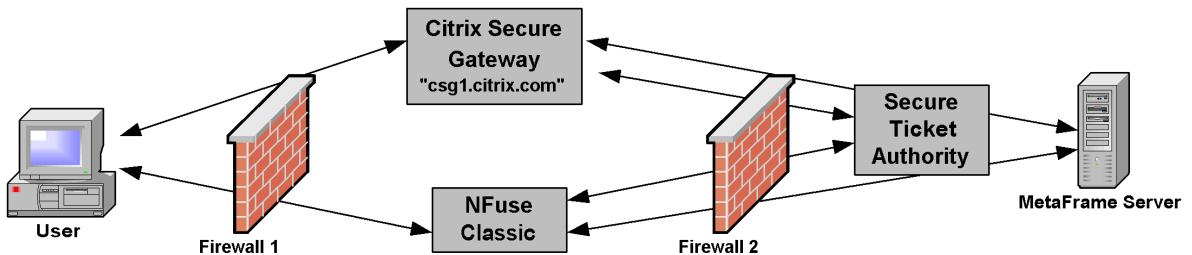
9. Choose whether to enable load balancing between Secure Ticket Authorities using the **Use the Secure Ticket Authority list for load balancing** check box. Enabling load balancing allows you to evenly distribute connections among servers so that no one server becomes overloaded. If an error occurs while communicating with a server, all further communication is load balanced between the remaining servers in the list.

Note NFuse Classic provides fault tolerance among servers in the Secure Ticket Authority list. If an error occurs while communicating with a server, the failed server is bypassed for the time specified in the **Bypass any failed server for** field in the **MetaFrame servers** page. See “Configuring Fault Tolerance” on page 50 for further information.

Example

This section provides an example of how to configure Citrix Secure Gateway support using the Admin tool.

In this example, you want to specify a Citrix Secure Gateway server called “csg1.citrix.com” on which ICA Clients use port 443, using the following Secure Ticket Authority address: <http://server1.citrix.com/scripts/CtxSta.dll>.



To configure NFuse Classic for Citrix Secure Gateway support:

1. Display the **Server-side firewall settings** page.
2. In **Default address translation setting** select **Citrix Secure Gateway**.
3. In the **Secure Gateway server** section, specify `csg1.citrix.com` in the **Address** field. This is the name of the server on the certificate.
4. In the **URL** field, edit the `<server>` part of template URL with `server1.citrix.com` and click **Add**.
5. Select the **Use the Secure Ticket Authority list for load balancing** check box to load balance connections between Secure Ticket Authority servers.
6. Click **Save** to save the changes.
7. Click **Apply Changes** in the **Apply changes** page.

Configuring Client-Side Firewall Settings

If you are using a SOCKS proxy server at the client-side of your NFuse Classic installation, you can configure whether or not clients must communicate with the MetaFrame server through the proxy server. You use the **Client-side firewall settings** page to do this.

A SOCKS proxy server positioned at the client-side of an NFuse Classic installation provides security benefits that include:

- Information hiding, where system names inside the firewall are not made known to systems outside the firewall through DNS (Domain Name System)
- Channeling different TCP connections through one connection

Using the Admin tool, you can set default SOCKS proxy rules for clients. However, you can also configure exceptions to this behavior for individual clients. To configure exceptions, you associate client addresses or partial addresses with a particular SOCKS proxy server address.

You can also specify that proxy behavior is controlled by the ICA Client. For example, to use the new Secure Proxy feature in Feature Release 2 for MetaFrame XP, configure NFuse Classic to use the proxy settings specified on the client, and configure the client for Secure Proxy. For more information about using clients to control proxy behavior, see the relevant *Citrix ICA Client Administrator's Guide*.

► **To configure default SOCKS proxy settings**

1. Display the **Client-side firewall settings** page.
2. Under **Default setting**, set **Use SOCKS proxy** to **Yes**.
3. Type the address of the SOCKS proxy server, as the ICA Client sees it, in the **Proxy address** field. This can be an IP address or DNS name.
4. In the **Proxy port** field, type the port number of the SOCKS proxy server. By default the port number is 1080.

► **To configure individual SOCKS proxy settings**

1. Display the **Client-side firewall settings** page.
2. Under **Specific SOCKS proxy settings**, type the client address in the **Client address prefix** field. You can enter the IP address of the client or the partial address of the client subnet.

Note If Web browsers connect to NFuse Classic through a proxy server or firewall that hides the client's IP address, the **Client address prefix** must specify the client address, as NFuse Classic sees it. For example, if a Web browser connects through a SOCKS proxy, specify the external address of the SOCKS proxy in the **Client address prefix**. This does not apply to Program Neighborhood Agent users.

3. Type the address of the SOCKS proxy server, as the ICA Client sees it, in the **Proxy address** field. You can specify an IP address or a DNS name.
4. If necessary, specify the port number of the SOCKS proxy server in the **Proxy port** field. By default the port number is 1080.
5. Click **Add**. The mapping is displayed in the **Mapping** list.
6. You can control the order in which multiple mappings are applied. Highlight a mapping and click the **Up** and **Down** buttons to place the mappings in order of priority.

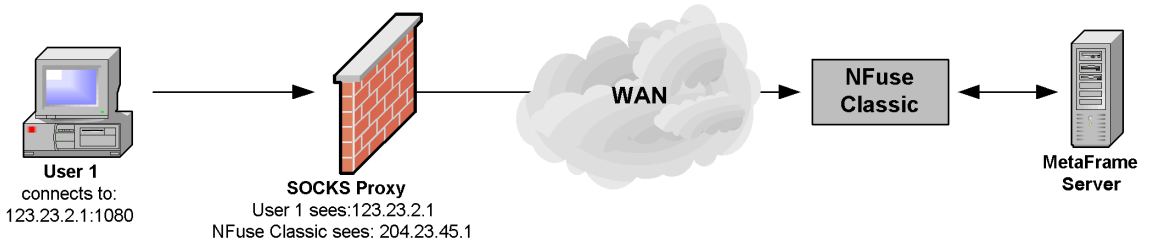
Tip To remove a mapping, highlight the mapping in the **Mapping** list and click **Remove**.

► **To control SOCKS proxy behavior using ICA Client proxy settings**

1. Display the **Client-side firewall settings** page.
2. Under **Default setting**, set **Use SOCKS proxy** to **No - use client proxy settings**.

Example

In this example, SOCKS proxy communication is configured for a user based at a satellite office.



Citrix MetaFrame and NFuse Classic are deployed to provide users with access to applications running on a MetaFrame server in the head office. However, there is also a user based at a satellite office who requires access to these applications. A SOCKS proxy server is used at this office to channel client communication. The user's Web browser connects through the SOCKS proxy, using address 123.23.2.1, and the proxy in turn connects to the MetaFrame server.

Configure NFuse Classic to associate the appropriate client address with the address of the SOCKS proxy server as follows:

1. Display the **Client-side firewall settings** page.
2. Under **Default setting**, set **Use SOCKS proxy** to **No - use client proxy settings**.
3. Under **Specific SOCKS proxy settings**, type the external address of the SOCKS proxy server as the NFuse Classic server sees it (204.23.45.1) in the **Client address prefix** field. The external address is used because the Web browser connects through a SOCKS proxy server that hides the client's IP address.
4. Type the address of the SOCKS proxy server, as the ICA Client sees it (123.23.2.1) in the **Proxy address** field.
5. Click **Add**. The mapping is displayed in the **Mapping** list.
6. Click **Save** to save the changes.
7. Click **Apply Changes** in the **Apply changes** page.

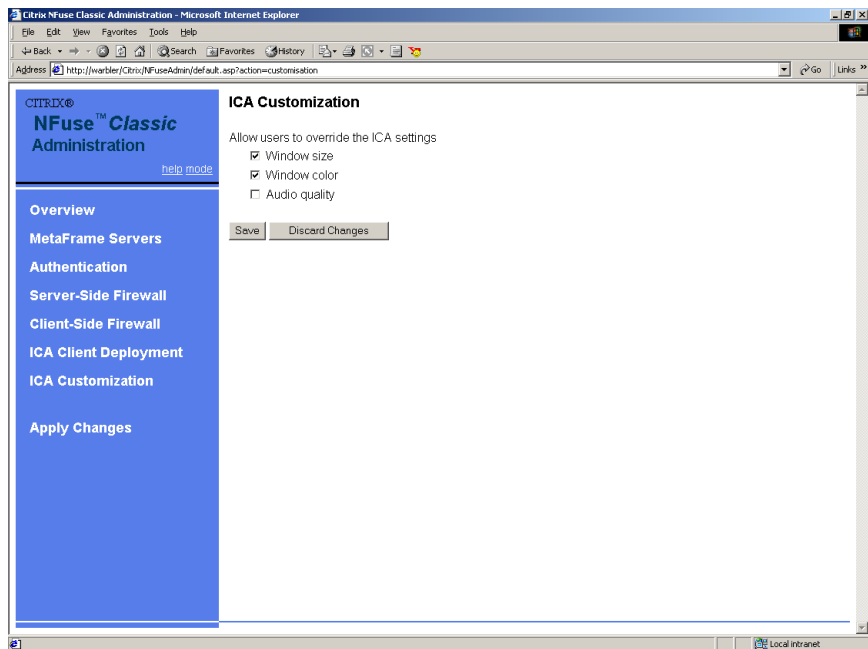
Allowing Users to Configure NFuse Classic Settings

You can specify the settings that users can adjust in their **Settings** page, using the **ICA Customization** page. You can specify whether users can adjust the:

- Window size of ICA sessions
- Color depth of ICA sessions
- Audio quality of ICA sessions

By default, users can adjust the window size of ICA sessions.

If you prevent users from adjusting a setting, the setting is not displayed in the **Settings** page in the users' presentation and the settings specified for the published application in the Citrix Management Console are used.



► **To specify the settings that users can adjust**

1. Display the **ICA Customization** page.
2. To allow users to adjust the window size, select **Window size**.
3. To allow users to adjust the color depth, select **Window color**.
4. To allow users to adjust the audio quality, select **Audio quality**.

Note To prevent users from accessing the **Settings** page, you must set the **AllowCustomizeSettings** parameter in the NFuse.conf file to **off**. When **AllowCustomizeSettings** is off, the Settings icon is not displayed to users. This means that users cannot access the Settings page to configure ICA session settings such as audio quality, window size, and color depth, and users cannot control display options including **Remember folder location**, **Show current folder location** and **Application Detail Display**, or configure **Embedded Client** options.

How User Settings are Stored on Client Devices

When users configure settings in NFuse Classic such as window size, their settings are stored as cookies on their client device. These settings are therefore remembered for all future applications launched using NFuse Classic. However, because the cookies are stored on the client device, users must access NFuse Classic from the same client device each time to use their settings.

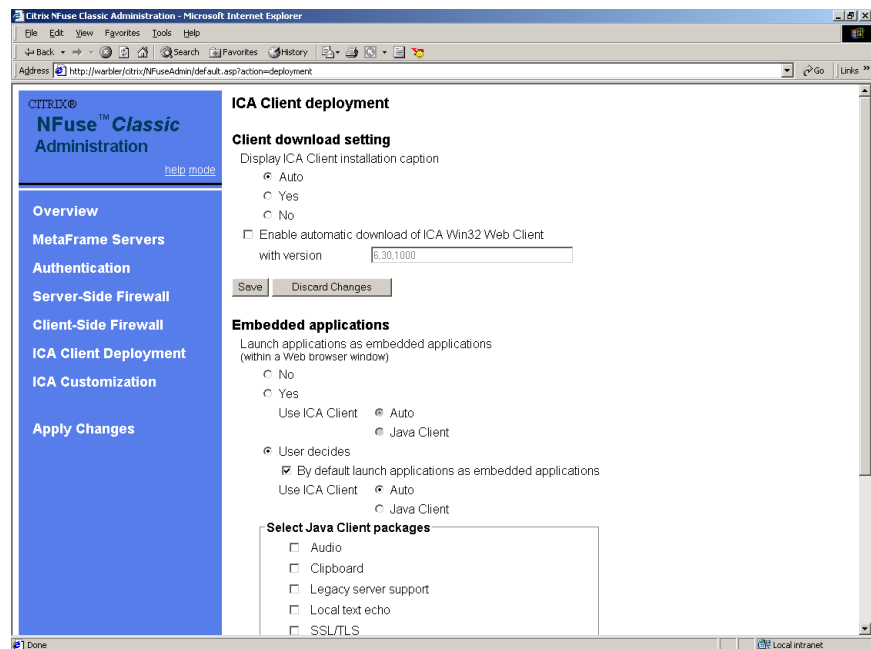
Depending on the operating system and Web browser used, these cookies may be specific to each user or all users will have the same settings. Customized settings made by guest users (logged on using the Guest User option) are not saved to the client device.

Configuring ICA Client Deployment

To use NFuse Classic, users must have a supported Web browser and ICA Client. One method of deploying ICA Clients to your users is with NFuse Classic's Web-based ICA Client installation feature.

You can configure the deployment of ICA Clients with NFuse Classic using the **ICA Client deployment** page. You can:

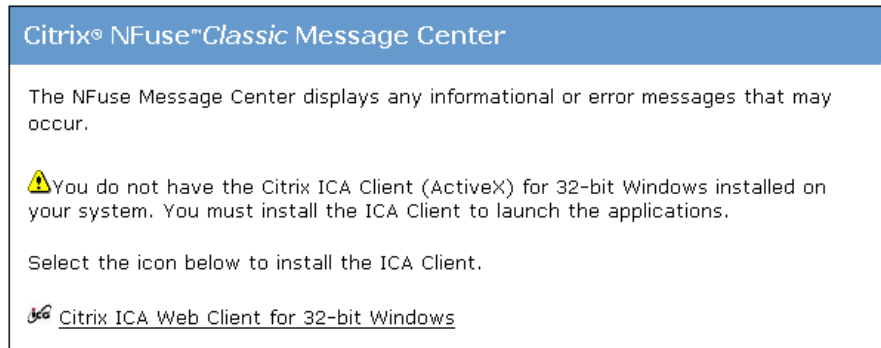
- Configure Web-based ICA Client installation. This feature allows you to easily deploy and install the appropriate ICA Clients on your users' devices using *installation captions*. Installation captions are links that are presented to users who require an ICA Client. Clicking on a link installs the ICA Client on the user's client device.
- Configure NFuse Classic to automatically deploy the smaller ICA Win32 Web Client installation file (Ica32t.exe) to your Windows users.
- Control whether applications are launched from, or embedded into, HTML Web pages. You can also enable users to choose how their applications are launched.
- Specify the components included in the ICA Java Client deployment or allow users to select the components that they require.



Configuring Web-Based ICA Client Installation

Web-based ICA Client installation allows you to easily deploy and install the appropriate ICA Clients on your users' devices.

If you enable this feature, when a user who requires an ICA Client visits an NFuse Classic site, NFuse Classic detects the user's client device and Web browser and presents the user with a link to the appropriate ICA Client installation file. When the user clicks on this link, the ICA Client is installed on the user's client device. The links presented to users are called *installation captions*. The following shows a typical installation caption:



By default, installation captions are displayed to users, but you can change this behavior using the **ICA Client deployment** page.

Note To use Web-based ICA Client installation, ensure your Web server contains the ICA Client installation files. For more information about Web-based ICA Client installation, see "ICA Clients and NFuse Classic" on page 109.

► To configure Web-based ICA Client installation

1. Display the **ICA Client deployment** page.
2. Under **Client download setting**, select one of the following settings:
 - **Auto.** On Windows platforms, if the user does not have an appropriate ICA Client installed, the installation caption is displayed. On other platforms the installation caption is always shown. This is the default setting.
 - **Yes.** The installation caption is always displayed on all platforms.
 - **No.** The installation caption is never displayed.

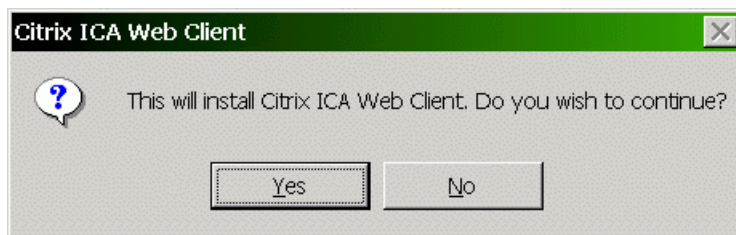
By default, Web-based ICA Client installation offers 32-bit Windows client devices the ICA Win32 Web Client installation file (Ica32t.exe). This client does not install the Program Neighborhood user interface and various other ICA Client components. Therefore, this client is smaller and easier to download so may be more suitable for users on low bandwidth connections. For more information about the features available in the Win32 Web Client, see the *ICA Win32 Client Administrator's Guide*.

To configure the ICA Clients offered to users by installation captions, you must edit the NFuse.conf file. For more information, see “Configuring Web-Based ICA Client Installation” on page 111 and “Configuring NFuse Classic Using NFuse.conf” on page 91.

Automatically Deploying the ICA Win32 Web Client

You can configure NFuse Classic to automatically deploy the ICA Win32 Web Client to your Windows users.

If you enable this feature, when a user accesses NFuse Classic, the user's client device and Web browser are detected. If the user is on a Windows platform and he or she does not have an ICA Client, or their current client is not up to date, NFuse Classic attempts to automatically install the ICA Win32 Web Client on the user's client device. The following prompt is displayed on the user's screen:



Each time a user visits the applications page, NFuse Classic checks to ensure the user's client is up to date and, if necessary, prompts the user to install the ICA Win32 Web Client.

► To enable automatic download of the ICA Win32 Web Client

1. Display the **ICA Client deployment** page.
2. Select the **Enable automatic download of ICA Win32 Web Client** check box.
3. Specify the version of the ICA Win32 Web Client to deploy. By default, this is Version 6,30,1000. Note that commas, rather than decimal points, are used as separators. Ensure your Web server contains this version of the ICA Win32 Web Client installation file.

Note Automatic installation of the ICA Win32 Web Client on Windows 2000 workstations requires the user to have administrative rights on the client device, or that the ActiveX control be registered in Active Directory. See Microsoft Technet article Q241163 for details.

Controlling the Launching and Embedding of Applications

Using the **ICA Client deployment** page, you can control whether applications are launched from or embedded into HTML pages.

If you choose to embed applications, you can specify the ICA Client that is used to launch the embedded application. You can deploy the ICA Win32 Client or the ICA Java Client depending on the user's platform, or you can use the ICA Java Client for all users. Alternatively, you can enable users to decide how their applications are launched using their **Settings** page.

This section provides information about launching and embedding applications and discusses the benefits associated with each of these methods. It also explains how to launch and embed applications using the Admin tool.

Embedded Applications

If you enable the launching of applications as embedded applications, the application runs in a Web browser window. The benefits of embedding applications include:

- If users do not have an ICA Client installed on their client device, you can specify the ICA Client that is used to launch the embedded application.
- Users have the same user experience, regardless of whether they are on a Windows or UNIX platform.
- Because you can enforce how the application is launched, training the user and supporting the application is easier, because the method of launching the application is fixed.

Non-Embedded Applications

If you choose not to embed applications, the application runs in a separate window on the local desktop. For this method to work, an ICA Client must be installed on the client device. If an ICA Client is not present, you can deploy ICA Clients on your users' devices using Web-based ICA Client installation. See "Configuring Web-Based ICA Client Installation" on page 83 for more information.

► **To control the launching and embedding of applications**

1. Display the **ICA Client deployment** page.
2. Configure how applications are launched as follows:
 - To embed applications into Web pages, select **Yes** in the **Embedded applications** section. Specify the ICA Client that will be used to launch the embedded application:
 - Choose **Auto** to automatically detect the user's client device and Web browser and deploy the appropriate ICA Client. If a Windows platform is detected, the ICA Win32 Web Client or Netscape plug-in is deployed, depending on the user's Web browser. NFuse Classic deploys the Java Client if it detects that the user is not on a Windows platform, or it is unable to detect the user's client device and Web browser.
 - Choose **Java Client** to force deployment of the ICA Java Client, regardless of the user's platform. The ICA Java Client can be configured to be a small download, so this option is best for users on low bandwidth connections. For more information about the ICA Java Client, see "About the ICA Java Client" on page 113 and the *Citrix ICA Java Client Administrator's Guide*.
 - To launch applications in a separate window on the local desktop (non-embedded applications), select **No** in the **Embedded applications** section. An ICA Client must be installed on the client device. If an ICA Client is not present, you can deploy ICA Clients on your users' devices using Web-based ICA Client installation. See "Configuring Web-Based ICA Client Installation" on page 83 for more information.
 - To enable users to decide how their applications are launched, select **User decides** in the **Embedded applications** section. When you enable this option, users can choose how their applications are launched in their **Settings** page. You can also specify what happens by default if users do not decide how their applications are launched, as follows:
 - To embed applications into Web pages by default, select the **By default launch applications as embedded applications** option. Specify the ICA Client that will be used to launch the embedded application. Select **Auto** to automatically detect the user's client device and Web browser and deploy the appropriate ICA Client. Select **Java Client** to force deployment of the ICA Java Client, regardless of the user's platform.
 - To launch applications in a separate window on the local desktop by default, deselect the **By default launch applications as embedded applications** option.

Customizing ICA Java Client Deployment

You can configure the components included in the deployment of the ICA Java Client in NFuse Classic.

You can configure the ICA Java Client to be a small download (as small as 300K) by removing unwanted functionality. For example, if you want to reduce the size of the download for users on low bandwidth connections, you can configure NFuse Classic to deploy only a minimum set of components. Alternatively, you can enable your users to control which components are required.

Note Some components that you make available in the ICA Java Client may require further configuration on the client device or on the MetaFrame server. For example, COM port mapping requires further configuration on the client device.

For more information about the ICA Java Client and its components, see “About the ICA Java Client” on page 113 and the *Citrix ICA Java Client Administrator's Guide*.

► To configure ICA Java Client deployment

1. Display the **ICA Client deployment** page.
2. Under the **Select Java Client packages** section, select the packages you want to include in the deployment. The following table explains the options available:

Package	Description
Audio	Enables applications running on the MetaFrame server to play sounds through a sound device installed on the client device. You can control the amount of bandwidth used by the client audio mapping on the server—see the appropriate <i>MetaFrame Administrator's Guide</i> for information.
Clipboard	Enables users to copy text and graphics between server-based applications and applications running locally on the client device.
Legacy server support	Allows users to connect to MetaFrame for Windows servers prior to MetaFrame XP (such as MetaFrame 1.8 and MetaFrame 1.0) and prior to Feature Release 1 of MetaFrame for UNIX Operating Systems.
Local text echo	Accelerates the display of the input text on the client device.
SSL/TLS	Secures communication using Secure Sockets Layer (SSL) and TLS (Transport Layer Security). SSL/TLS provides server authentication, encryption of the data stream, and message integrity checks.
Encryption	Provides strong encryption to increase the privacy of ICA connections.

Package	Description
Client drive mapping	<p>Enables users to access their local drives from within an ICA session. When users connect to the MetaFrame server, their client drives are automatically mounted, such as floppy disks, network drives, and CD-ROM drives. Users can access their locally stored files, work with them during their ICA sessions, and save them again on a local drive or on a drive on the MetaFrame server.</p> <p>To enable this setting, users must also configure client drive mapping in the ICA Java Client Settings dialog. See the <i>Citrix ICA Java Client Administrator's Guide</i> for more information.</p>
COM port mapping	<p>Allows devices attached to the client device's COM ports to be used during an ICA session on the MetaFrame server. These mappings can be used by applications in the same way as other network mappings.</p> <p>This feature requires third-party software to be installed on the client device. See the <i>Citrix ICA Java Client Administrator's Guide</i> for more information.</p>
Printer mapping	<p>Enables users to print to their local or network printers from within an ICA session.</p>
Configuration UI	<p>Enables the ICA Java Client Settings dialog. This dialog can be used by users to configure the ICA Java Client.</p>

3. To allow users to control which Java Client packages are enabled, select the **Allow user to choose packages** check box. When you select this option, users can control some of the packages listed in the table above, using their **Settings** page.

Tip You can configure these and many other properties of the ICA Java Client. See the *Citrix ICA Java Client Administrator's Guide* for more information.

Configuring Communication With Enterprise Services for NFuse

To use Enterprise Services for NFuse in your NFuse Classic installation, you must configure NFuse Classic to communicate with the Enterprise Services for NFuse server. Enterprise Services for NFuse extends NFuse Classic's capabilities, allowing you to deploy applications to users from multiple MetaFrame farms.

Use the **mode** link in the NFuse Classic Admin tool to switch to Enterprise Services mode. This mode is a global setting that causes NFuse Classic to communicate with an Enterprise Services for NFuse server, rather than with MetaFrame servers running the Citrix XML Service.

However, when you enable this mode, the interaction between NFuse Classic and Enterprise Services for NFuse changes the way in which some NFuse Classic features work. These changes are described below.

Important Set Enterprise Services mode only if you want NFuse Classic to communicate with an Enterprise Services for NFuse server. This mode alters NFuse Classic's behavior to allow it to interact with Enterprise Services for NFuse. As a result, some settings in NFuse Classic are overridden by Enterprise Services for NFuse.

For more information about using Enterprise Services for NFuse, see the *Citrix Enterprise Services for NFuse Administrator's Guide*.

Changes to NFuse Classic Features

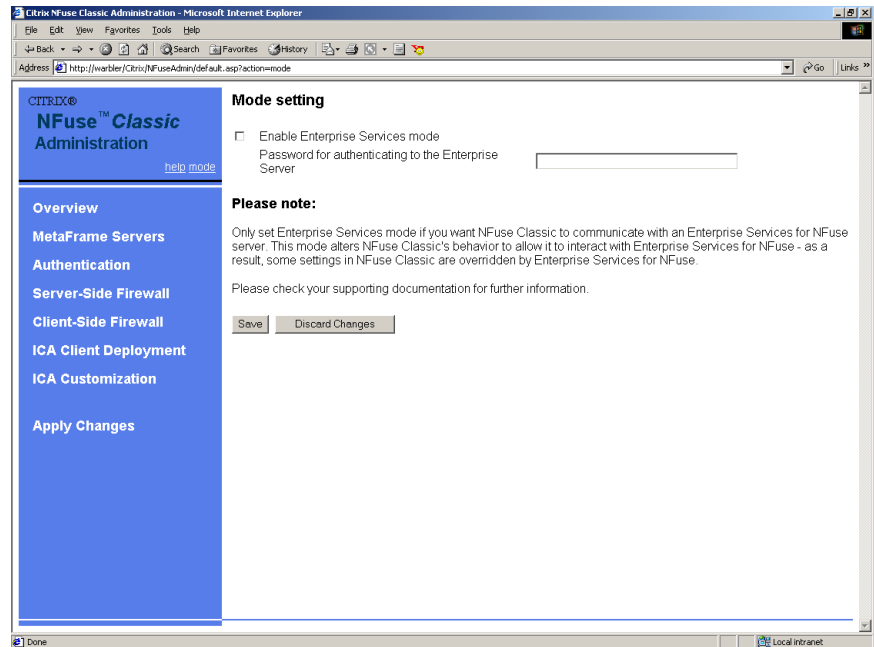
When you enable Enterprise Services mode some NFuse Classic features are not supported, or work differently in Enterprise Services for NFuse. The features affected are:

- Load balancing between servers running the Citrix XML Service no longer applies, because NFuse Classic now communicates with an Enterprise Services for NFuse server.
- Alternate addressing works differently in Enterprise Services for NFuse. See the *Citrix Enterprise Services for NFuse Administrator's Guide* for information.
- Firewall support. For more information about the effects, see the *Citrix Enterprise Services for NFuse Administrator's Guide*.
- The use of embedded ICA Clients, auto-deployment of the ICA Win32 Web Client, and customization of ICA Java Client packages are not supported, because these options are not displayed in the Enterprise Services for NFuse user presentation.

- The feature that allows users to change their passwords works differently in Enterprise Services for NFuse. Enterprise Services for NFuse does not allow the administrator to control whether users can change their login passwords.
- Smart card support and pass-through authentication are supported but must be configured using the Enterprise Services for NFuse Admin tool.

► **To set Enterprise Services for NFuse mode**

1. Click the **mode** link in the Admin tool. The **Mode setting** page appears.



2. Select the **Enable Enterprise Services mode** check box.
3. To allow Desktop Credential Pass-Through and smart card authentication between NFuse Classic and Enterprise Services for NFuse, type a password in the **Password for authenticating to the Enterprise Server** field. Enterprise Services for NFuse checks this password to authenticate the NFuse Classic server.

Note The password must also be configured in Enterprise Services for NFuse. See the *Citrix Enterprise Services for NFuse Administrator's Guide* for further information.

Configuring NFuse Classic Using NFuse.conf

NFuse Classic includes a configuration file, called `NFuse.conf`, that lets you change several of NFuse Classic's properties. You can use this file to perform day to day administration tasks and customize many more settings. For example, you can use `NFuse.conf` to specify the settings that users can adjust on the Settings page or configure user authentication to NFuse Classic.

The `NFuse.conf` file is available on all platforms in the software directory. On Windows this is typically: `C:\Program Files\Citrix\NFuse\Conf`; on UNIX systems, this may be: `/usr/local/tomcat/webapps/Citrix/WEB-INF`.

The settings in `NFuse.conf` are global. Therefore, all Web pages generated by NFuse Classic draw from this file's values, so changes made to `NFuse.conf` affect all Web pages served by NFuse Classic. However, you can override some values in `NFuse.conf` on a per-page basis in your Web server scripts. For more information about Web server scripts, see the *Customizing NFuse Classic guide*.

Important For changes made to `NFuse.conf` to take effect, you must stop and restart the NFuse Classic server. For Microsoft Internet Information Server (IIS) version 4.0, 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. For Microsoft Internet Information Server (IIS) version 5.0, use the command-line utility `IISRESET` to restart the IIS Admin Service and all of its dependent services.

The following table shows the parameters that `NFuse.conf` can contain (in alphabetical order). If a parameter is not specified in `NFuse.conf`, its default value is used.

Parameter	Default Value	Description
AddressResolutionType	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 available only 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>
AllowCustomizeAudio	off	Specifies whether users can adjust the audio quality for ICA sessions from the Settings page. See AllowCustomizeSettings for more information.
AllowCustomizeEmbedApplications	off	<p>Enables users to decide how their applications are launched. The options are:</p> <p>on—allows users to override the EmbedApplications and EmbedMethod fields and choose how their applications are launched. If you enable this option but the users do not choose how to launch their applications, the default values for EmbedApplications and EmbedMethod are used.</p> <p>off—does not allow users to choose how their applications are launched.</p>
AllowCustomizeJavaClientPackages	off	<p>Allows users to control which ICA Java Client packages are enabled. The options are:</p> <p>on—allows users to control which Java Client packages are enabled</p> <p>off—does not allow users to control which Java Client packages are enabled</p>
AllowCustomizeSettings	on	<p>Enables user access to the Settings page. The options are:</p> <p>on—allows users access to the Settings page</p> <p>off—does not allow users access to the Settings page</p> <p>The Settings page contains 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 (such as AllowCustomizeWin Size), if the value is set to on, users can edit the setting on the Settings page. If the value is off, the setting is not displayed in the 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 guests are not saved to the client device.</p>
AllowCustomizeWinColor	off	Specifies whether users can adjust the color depth for ICA sessions from the Settings page. See AllowCustomizeSettings for more information.
AllowCustomizeWinSize	on	Specifies whether users can adjust the window size for ICA sessions from the Settings page. See AllowCustomizeSettings for more information.

Parameter	Default Value	Description
AllowUserPassword Change	never	<p>Specifies whether users are permitted to change their logon passwords within an NFuse Classic session. The options are:</p> <p>never—users cannot change their logon password within NFuse Classic</p> <p>always—users can change their password as often as they want in NFuse Classic. When you enable this option, the change password icon appears on the user's screen. When users click on this icon, the change password dialog box appears, where users can enter a new password.</p> <p>expired-only—users can change their password only when the password expires. When a user fails to log on to NFuse Classic due to an expired password, the user is automatically redirected to the change password dialog. After changing the password, the user is automatically logged on to NFuse Classic using the new password.</p>
AlternateAddress	off	<p>Specifies whether to replace the address of the specified MetaFrame server with its alternate address in the .lca files sent to client devices to launch ICA sessions. The options are:</p> <p>on—The external address of MetaFrame servers is included in .lca files generated by NFuse Classic.</p> <p>off—No alternate address translation is performed.</p> <p>mapped—The address depends upon the mappings you set in ClientAddressMap.</p> <p>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> or the ctxalt command in the <i>MetaFrame for UNIX Operating Systems Administrator's Guide</i>.</p>

Parameter	Default Value	Description
AuthenticationMethods	Explicit	<p>Specifies the ways in which users can authenticate to NFuse Classic. Authentication to NFuse Classic occurs when a user initially logs on to NFuse Classic, either using the Login dialog or by another authentication method. The options are:</p> <p>Explicit—Users must have a user account and must supply a username and password to log on to NFuse Classic.</p> <p>Guest—Enables guest users to log on to NFuse Classic using the Guest User option displayed in the user Login page. Guest users do not have to supply a username or password, and can access applications that the MetaFrame administrator has published for anonymous use.</p> <p>Integrated—Enables Desktop Credential Pass-Through. This allows users to authenticate to NFuse Classic using the credentials they provided when they logged on to their Windows desktop. Users do not need to enter credentials at the NFuse Classic Login page and their NFuse Classic application set is automatically displayed. For this feature to work, NFuse Classic must be running on IIS and users must be running Internet Explorer Version 5.0 or later, on Windows 2000 or later.</p> <p>Certificate—Allows users to authenticate to NFuse Classic by inserting a smart card in a smart-card reader attached to the client device. Smart cards eliminate the need for users to remember multiple sign on processes, user ids, and passwords. This feature is available only on Windows/IIS and users must be running Internet Explorer Version 5.0 or later on Windows 2000 or later.</p> <p>To specify more than one authentication method, use commas to separate the list—for example: Explicit,Guest</p>
AutoDeployWebClient	off	<p>Specifies whether to automatically deploy the ICA Win32 Web Client to your Windows users. The options are:</p> <p>on—Attempts to automatically install the ICA Win32 Web Client if NFuse Classic detects that a Windows user does not have an ICA Client installed or the ICA Client is not up to date.</p> <p>off—Does not attempt to automatically install the ICA Win32 Web Client. Ensure that ICA Clients are available in the wwwroot\Citrix\ICAWEB folder.</p>
BypassFailedServer Duration	60	<p>Specifies the length of time, in minutes, for which a failed MetaFrame server is bypassed. If an error occurs while communicating with a server, the failed server is bypassed for this time and communication continues with the remaining servers in the SessionField.NFuse_CitrixServer list.</p> <p>Note that this field also controls the length of time that a failed Citrix Secure Gateway Secure Ticket Authority server is bypassed for.</p>
CacheExpireTime	3600	<p>Specifies the default expiration timeout value in seconds for the AppDataList objects stored in the AppListCache object. Used for caching of application set information on the Web server. See the descriptions of example NFuse Classic Web pages in the <i>Customizing NFuse Classic Guide</i> for more information about application caching.</p>

Parameter	Default Value	Description
ClientAddressMap	none	<p>Configures NFuse Classic to supply the appropriate IP address, depending upon the client address. For example, if network address translation is enabled at the firewall, you can specify that clients outside the firewall are supplied with an alternate address.</p> <p>ClientAddressMap consists of: <ClientAddress>,<AddressType>,... where: <i>ClientAddress</i> is the IP address or partial IP address (IP address prefix) of the client. Note that subnet masks and asterisks used as wildcards (such as 10.*.128.12.) are not supported. However, a single asterisk can be used to denote “any address”.</p> <p><i>AddressType</i> is “normal”, “alternate”, “translated” or “csg”, where: normal is the actual address of the MetaFrame server alternate means the alternate address is supplied. The MetaFrame server must be configured with an alternate address and the firewall configured for network address translation translated means the ServerAddressMap field is used to determine the appropriate IP address csg means Citrix Secure Gateway is used to protect incoming connections.</p>
DefaultClient	on	<p>Specifies whether to display all ICA Clients available to download in the installation caption, when NFuse Classic is unable to detect the user’s client device and Web browser. This setting is relevant only when ShowClientInstallCaption is set to on or auto. The options are:</p> <p>on—Displays only the default ICA Client in the installation caption. off—Displays all ICA Clients available to download in the installation caption.</p> <p>For example: on Windows, if DefaultClient=On the ICA Win32 Program Neighborhood Client is offered (ica32.exe). If DefaultClient=Off all the following are offered: ICA Win32 Web Client, ICA Win32 Program Neighborhood Client and the ICA Java Client.</p>
DTDDirectory	N/A	<p>Specifies the directory containing the NFuse Classic DTD file. The default is the Java Virtual Machine’s working directory.</p>
EmbedApplications	off	<p>Specifies whether applications are launched from, or embedded into, HTML Web pages. The options are:</p> <p>on—applications are embedded into Web pages off—applications are not embedded; instead, the application runs in a separate window on the local desktop. If an ICA Client is not present, you can deploy ICA Clients on your users’ devices using Web-based ICA Client installation.</p>

Parameter	Default Value	Description
EmbedMethod	auto	<p>If you set EmbedApplications to on to embed applications into Web pages, use this field to specify the ICA Client that will be used to launch the embedded application. The options are:</p> <p>auto—NFuse Classic automatically detects the user's client device and Web browser and deploys the appropriate ICA Client. If a Windows platform is detected, the ICA Win32 Web Client or Netscape plug-in is deployed, depending on the user's Web browser. NFuse Classic deploys the ICA Java Client if it detects that the user is not on a Windows platform, or it is unable to detect the user's client device and Web browser.</p> <p>JavaClient—forces deployment of the ICA Java Client, regardless of the user's platform. ICA Java Client deployment is smaller than Win32 deployment, so this option is best for users on low bandwidth connections.</p>
EnableServerLoad Balancing	on	<p>Enables load balancing between servers running the Citrix XML Service. Load balancing allows you to evenly distribute connections among these servers so that no one server becomes overloaded.</p> <p>If an error occurs while communicating with a server, all further communication is load balanced among the remaining servers in the list. The failed server is bypassed for a specific time period (by default, 60 minutes) but you can change this using BypassFailedServerDuration.</p>
EnableSTALoad Balancing	on	<p>Enables load balancing between Secure Ticket Authority servers. Load balancing allows you to evenly distribute connections among these servers so that no one server becomes overloaded. If an error occurs while communicating with a server, all further communication is load balanced among the remaining servers in the list.</p>
ForceLoginDomain	none	<p>When using Microsoft domain-based authentication, you can force all users to log on 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 Classic Login page. When a value is specified, the domain is not displayed to users on the NFuse Classic Login page.</p> <p>When using ADS 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>
HpUxUnixClient	default	<p>Specifies captions and links for HP-UX Client platforms. See the description for Win32Client for information about specifying custom links.</p>
HttpInputEncoding	UTF-8	<p>Specifies the encoding used for incoming HTTP such as form data. Do not edit this parameter.</p>
HttpOutputEncoding	UTF-8	<p>Specifies the encoding used for outgoing HTTP such as HTML pages that display application sets. Do not edit this parameter.</p>
IbmAixClient	default	<p>Specifies captions and links for IBM-AIX Client platforms. See the description for Win32Client for information about specifying custom links.</p>

Parameter	Default Value	Description
JavaClientPackages	PrinterMapping, ConfigUI, SecureICA	<p>Specifies the packages included in the deployment of the Java Client. For example, if you want to reduce the size of the Java Client deployment for users on low bandwidth connections, you can configure NFuse Classic to deploy a minimum set of components. The available packages are:</p> <p>Audio—Enables applications running on the MetaFrame server to play sounds through a sound device installed on the client computer.</p> <p>ClientDriveMapping—Enables users to access their local drives from within an ICA session. Users can access locally stored files, work with them during their ICA sessions, and save them again on a local drive or on a drive on the MetaFrame server. To enable this setting, your users must also configure client drive mapping in the ICA Java Client Settings dialog.</p> <p>Clipboard—Enables users to copy text and graphics between server-based applications and applications running locally on the client device.</p> <p>COMPortMapping—Allows devices attached to the client computer's COM ports to be used during an ICA session on the MetaFrame server. These mappings can be used by applications in the same way as other network mappings. This feature requires 3rd party software to be installed on the client device.</p> <p>ConfigUI—Enables the ICA Java Client Settings dialog, which can be used by users to configure the ICA Java Client.</p> <p>PrinterMapping—Enables users to print to their local or network printers from within an ICA session.</p> <p>SecureICA—Provides strong encryption to increase the privacy of ICA connections.</p> <p>Thinwire1—Allows users to connect to MetaFrame for Windows servers prior to MetaFrame XP (such as MetaFrame 1.8 and MetaFrame 1.0) and prior to Feature Release 1 of MetaFrame for UNIX Operating Systems.</p> <p>ZeroLatency—Accelerates the display of the input text on the client device.</p> <p>SSL—Secures communication using Secure Sockets Layer (SSL) and TLS (Transport Layer Security). SSL/TLS provides server authentication, encryption of the data stream, and message integrity checks.</p> <p>See the <i>Citrix ICA Java Client Administrator's Guide</i> for more information about these features.</p> <p>To specify more than one package, use commas to separate the list—for example: Audio,ClientDriveMapping,Clipboard</p>
LinuxClient	default	<p>Specifies captions and links for Linux Client platforms. See the description for Win32Client for information about specifying custom links.</p>

Parameter	Default Value	Description
LoginType	default	<p>Specifies Microsoft domain-based authentication, NDS authentication or UNIX-based authentication. The options are:</p> <p>default—Use Microsoft domain-based authentication or UNIX-based authentication.</p> <p>nds—Use Novell NDS authentication. To use NDS authentication, you must also specify an NDS tree using the NDSTreeName parameter. NDS authentication is supported on Windows IIS/ASP only, because this requires native Win32 Novell NetWare Client DLLs to perform the look-up for the context search.</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 the <i>Citrix ICA Win32 Client Administrator's Guide</i> for more information about editing the Config.xml file.</p>
MacClient	default	Specifies captions and links for Macintosh Client platforms. See the description for Win32Client for information about specifying custom links.
NDSTreeName	none	Specifies the NDS tree to use for authenticating users when using NDS authentication. By default, this parameter is commented out by a pound symbol or hash mark (#) at the beginning of the line.
NFuseEnterpriseMode	off	<p>Use this to switch Enterprise Services mode on or off. This mode is a global setting that causes NFuse Classic to communicate with an Enterprise Services for NFuse server, rather than with MetaFrame servers running the Citrix XML Service. When you enable this mode, the interaction between NFuse Classic and Enterprise Services for NFuse changes the way in which some NFuse Classic features work. See “Changes to NFuse Classic Features” on page 89 for more information about the features affected.</p> <p>Note: Set Enterprise Services mode only if you want NFuse Classic to communicate with an Enterprise Services for NFuse server.</p>
NFuseEnterprise Password		<p>When NFuse Classic is switched to Enterprise Services mode using NFuseEnterpriseMode, use this to specify the password passed from NFuse Classic to Enterprise Services for NFuse. This password is used for Desktop Credential Pass-Through and smart card authentication between NFuse Classic and Enterprise Services for NFuse. This password must also be configured in Enterprise Services for NFuse. See the <i>Citrix Enterprise Services for NFuse Administrator's Guide</i> for further information.</p>
OtherClient	default	Specifies captions and links for unrecognized client platforms. The default behavior is to display a message telling the user that there is no support for the client platform. See the description for Win32Client for information about specifying custom links.

Parameter	Default Value	Description
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>"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>Select the icon below to install the ICA Client."</p>
PooledSockets	on	<p>Specifies whether to use socket pooling or not.. When socket pooling is enabled, NFuse maintains a pool of sockets, rather than creating a socket each time one is needed and returning it to the operating system when the connection is closed. Enabling socket pooling enhances performance. The options are:</p> <p>on—Enable socket pooling to enhance performance.</p> <p>off—Disable socket pooling.</p>
RequestICAClient SecureChannel	Detect-AnyCiphers	<p>Specifies Secure Sockets Layer (SSL), Transport Layer Security (TLS) and ciphersuite preferences, when Citrix SSL Relay or Citrix Secure Gateway are used to secure ICA traffic. Some ICA Clients support both TLS and SSL to secure ICA traffic to MetaFrame servers. You can use this setting to request that ICA Clients use TLS in preference to SSL. Note that NFuse Classic does not enforce the use of TLS. The options are:</p> <p>Detect-AnyCiphers—ICA Clients can use TLS, SSL with any ciphersuite.</p> <p>TLS-GovCiphers—Requests ICA Clients to use TLS with Government ciphersuites.</p> <p>SSL-AnyCiphers—Requests ICA Clients to use SSL using any ciphersuite.</p>
RetryCount	5	<p>Specifies the number of times a failed request to the Citrix XML Service is retried before the Service is deemed to have failed.</p>
RequestPassThru	auto	<p>Specifies whether or not pass-through authentication can be used to authenticate to MetaFrame. Authentication to MetaFrame occurs when a user clicks a hyperlink to launch an application. The options are:</p> <p>auto—If the user authenticated to NFuse Classic using Desktop Credential Pass-Through, NFuse Classic attempts to authenticate to MetaFrame using this method. This is the default. See AuthenticationMethods for information about Desktop Credential Pass-Through.</p> <p>on—NFuse Classic always attempts to authenticate to MetaFrame using pass-through authentication.</p> <p>off—NFuse Classic never attempts to authenticate to MetaFrame using pass-through authentication.</p>
ScoUnixClient	default	<p>Specifies captions and links for SCO UNIX Client platforms. See the description for Win32Client for information about specifying custom links.</p>

Parameter	Default Value	Description
SearchContextList	none	Configures context lookup for NDS authentication. Set this value to a comma-delimited list of context names, so 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 NDS tree. By default, this parameter is commented out by a pound symbol or hash mark (#) at the beginning of the line.
ServerAddressMap	none	<p>Configures NFuse Classic to supply the appropriate IP address, depending upon the mappings you specify.</p> <p>ServerAddressMap consists of: <NormalAddress>,<TranslatedAddress>,... where:</p> <p><i>NormalAddress</i> is the actual address of the MetaFrame server. This can be an IP address or FQDN, with or without a port number. The value of AddressResolutionType determines whether the normal MetaFrame server address must be a FQDN or IP address. If AddressResolutionType is set to DNS-port or DNS, all normal addresses must be FQDNs; if it is set to IPv4-port or IPv4, all normal addresses must be IP addresses. If you do not specify a port number, port 1494 is used by default.</p> <p><i>TranslatedAddress</i> is the translated (external) IP address that clients must use to connect to the MetaFrame server. This can be an IP address or FQDN, with or without a port number. If you do not specify a port number, port 1494 is used by default.</p>
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>

Parameter	Default Value	Description
SessionField.NFuse_CitrixServer	N/A	<p>Specifies the name of one or more MetaFrame servers in the farm running the Citrix XML Service. The XML Service is the communication link between the server farm and the Web server. The default value is the server name entered during NFuse Classic installation. The server name can be a Windows NT server name, IP address, or DNS name. If you specify more than one server, use commas to separate the list; for example: server1,server2, ...</p> <p>If an error occurs while communicating with a server, the failed MetaFrame server is bypassed by NFuse Classic for the length of time specified in BypassFailedServerDuration, and communication continues with the remaining servers in the list.</p> <p>If you are using a secure connection (for example, you set the SessionField.NFuse_Transport field to SSL or HTTPS) ensure the name you specify in NFuse_CitrixServer matches the name on the MetaFrame server's certificate.</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>All MetaFrame servers in the farm must have the Citrix XML Service configured on this port.</p>
SessionField.NFuse_ContentType	text/html	Sets the MIME type of pages produced by the NFuse Classic Java objects to the specified value. The default value is text/html.
SessionField.NFuse_CSG_AddressTranslation	normal	<p>Use this field to configure Citrix Secure Gateway support. Set this to alternate if network address translation is enabled on a firewall between the Secure Gateway server and the MetaFrame server, and the MetaFrame server is configured for network address translation.</p> <p>Set this to normal if no address translating firewall is present.</p>
SessionField.NFuse_CSG_Enable	off	Use this field to enable Citrix Secure Gateway support. This must be set to On or the other Secure Gateway configuration settings are ignored.
SessionField.NFuse_CSG_Server	none	Use this field to configure Citrix Secure Gateway support. This specifies the Fully Qualified Domain Name (FQDN) of the Citrix Secure Gateway server that ICA Clients must use. This name must match the name of the server on the certificate.
SessionField.NFuse_CSG_ServerPort	443	Use this field to configure Citrix Secure Gateway support. This specifies the port number on the Gateway server that ICA Clients must use.
SessionField.NFuse_CSG_STA_URLn	N/A	Use this field to configure Citrix Secure Gateway support. This specifies the address of up to 256 Secure Ticket Authorities that NFuse Classic can use, where <i>n</i> is a number from 1 to 256. Each URL must begin with "http://". For example: http://servername/scripts/CtxSTA.dll

Parameter	Default Value	Description
SessionField.NFuse_IconCache	/NFuselcons/	Specifies the directory used to store NFuse Classic-generated application icon files (.Gif). The default value is /NFuselcons/. 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_RelayServerPort	none	Specifies the TCP port of the SSL Relay. By default, this parameter is not included in the NFuse.conf file.
SessionField.NFuse_Template	none	Specifies the name of the default ICA template file.
SessionField.NFuse_TemplatesDir	N/A	Specifies the directory where a TemplateParser object looks when a template file is specified with the NFuse_Template session field.
SessionField.NFuse_TemplatesURL	none	URL of the directory where the ICA template files are located.
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.
SessionField.NFuse_Transport	HTTP	<p>Specifies the protocol used to transport NFuse Classic data between the Web server and the MetaFrame server specified in NFuse_CitrixServer. The options are:</p> <p>HTTP—Use this option to send the data over a standard HTTP connection to the server and port specified in NFuse_CitrixServer and NFuse_CitrixServerPort.</p> <p>SSL—Use this option to send data over a secure connection that uses a MetaFrame 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 the Citrix SSL Relay server specified in NFuse_RelayServerPort.</p> <p>HTTPS— Use this option to send data over a secure HTTP connection using SSL, to the server specified in NFuse_CitrixServer and NFuse_CitrixServerPort.</p>
SgiUnixClient	default	Specifies captions and links for SGI UNIX Client platforms. See the description for Win32Client for information about specifying custom links.
ShowClientInstallCaption	auto	<p>Specifies whether Web-based ICA Client installation captions are displayed to users. The options are:</p> <p>auto—on Windows platforms, if the user does not have an ICA Client installed, an installation caption is displayed. On other platforms the installation caption is always shown. This is the default setting.</p> <p>on—the installation caption is always displayed, on all platforms.</p> <p>off—the installation caption is never displayed.</p> <p>See the description for Win32Client for information about customizing the installation captions and download links.</p>

Parameter	Default Value	Description
SmartCardToMF	auto	<p>Specifies whether smart cards can be used to authenticate to MetaFrame. Authentication to MetaFrame occurs when a user clicks on a hyperlink to launch an application. The options are:</p> <p>auto—This is the default. If the user authenticated to NFuse Classic using a smart card, NFuse Classic attempts to authenticate to MetaFrame using this method. If RequestPassThru is set to on, the ICA Client does not pass the PIN to the MetaFrame server (this means the user is prompted for a PIN).</p> <p>on—NFuse Classic always attempts to authenticate to MetaFrame using smart card credentials. If RequestPassThru is set to on, the ICA Client passes the PIN to the MetaFrame server (this means the user is not prompted for a PIN).</p> <p>off—NFuse Classic never attempts to authenticate to MetaFrame using smart card credentials.</p>
SOCKSProxy	none	<p>Configures SOCKS proxy rules for clients. You can configure NFuse Classic to use specific proxy server addresses for particular clients. To do this, you associate a SOCKS proxy server address with a client address or client subnet address.</p> <p>The SOCKSProxy mapping consists of: <i><ClientAddress>,<ProxyAddress>,...</i> where:</p> <p><i>ClientAddress</i> is the IP address of the client (this can be a partial address used to match subnets, a specific IP address, or an * (asterisk) wildcard to match any address).</p> <p>Note that if Web browsers connect to NFuse Classic through a proxy server or firewall that hides the client's IP address, the <i>ClientAddress</i> must specify the client address as NFuse Classic sees it. This does not apply to Program Neighborhood Agent users.</p> <p><i>ProxyAddress</i> is the address of the proxy server to be used by the client. This can be an IP address or DNS name, with or without a port number. If you do not specify a port number, port 1080 is used by default.</p>
SolarisUnixClient	default	Specifies captions and links for Solaris Client platforms. See the description for Win32Client for information about specifying custom links.
SslKeystore	N/A	Specifies the directory containing the certificate authority root certificates. NFuse Classic uses root certificates when authenticating a Citrix SSL Relay server.
StaticStringTextFile	N/A	<p>Specifies the path to the static string file; for example: D:\WINNT\java\trustlib\nfuse.txt. This file contains all of the text used by NFuse Classic.</p> <p>Note: Editing the nfuse.txt file is not supported.</p>
StaticStringTextFile Encoding	8859_1	Specifies the encoding used for the static string file.
TemplateFileEncoding	8859_1	Specifies the encoding used for Citrix HTML template files.

Parameter	Default Value	Description
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.
Tru64Client	default	Specifies captions and links for Tru64 UNIX Client platforms. See the description for Win32Client for information about specifying custom links.
URLMapping./	N/A	Specifies the path to your Web server's Web publishing root directory. For example, in a typical Microsoft Internet Information Server system, this is: C:\inetpub\WWWRoot.
Version	1.7	Do not edit this parameter.
WebClientVersion	6,30,1000	Specifies the version number of the ICA Win32 Web Client to deploy.
Win16Client	default	Specifies captions and links for 16-bit Windows Client platforms. See the description for Win32Client for information about specifying custom links.
Win32Client	default	<p>Specifies captions and links for 32-bit Windows Client platforms.</p> <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,..., and so on, where caption is the display text and url is the URL for the ICA Client. The caption is shown in the Message Center of the NFuse Classic Login page as a hyperlink to the specified URL.</p>

Examples

This section provides typical examples of how to configure NFuse Classic using the NFuse.conf file.

Configuring Communication with MetaFrame

In this example, you want to specify the name of an additional MetaFrame server running the Citrix XML Service. The XML Service acts as a communication link between the server farm and the NFuse Classic server.

Communication is currently with the server “marx”, but you want to add the server “engels” in case marx fails. To do this:

1. Locate the following line in NFuse.conf:
`SessionField.NFuse_CitrixServer=marx`
2. Edit this line to include the additional server, as follows:
`SessionField.NFuse_CitrixServer=marx,engels`
3. Restart the Web server to apply the changes.

Configuring SSL Relay Communication

In this example, you want to secure communication between the Web server and the MetaFrame server, using Secure Sockets Layer (SSL). Citrix SSL Relay is installed on a MetaFrame server that has a FQDN of “www.hegel.company-name.com”. SSL Relay listens for connections on TCP port 443.

Communication is currently with the server “marx”, but you want to replace marx with www.hegel.company-name.com. To do this:

1. Open NFuse.conf and locate the following lines:
`SessionField.NFuse_CitrixServer=marx`
`SessionField.NFuse_Transport=HTTP`
`#SessionField.NFuse_RelayServerPort=`

Note `SessionField.NFuse_RelayServerPort` is not included in the NFuse.conf file by default, so you may need to add this line to NFuse.conf. The line may be commented out using a “#”; if it is commented out, remove the “#” symbol from the start of the line.

2. Edit these lines as follows:
`SessionField.NFuse_CitrixServer=www.hegel.company-name.com`
`SessionField.NFuse_Transport=SSL`
`SessionField.NFuse_RelayServerPort=443`

Note The server name specified in SessionField.NFuse_CitrixServer must match the name on the server's certificate.

3. Restart the Web server to apply the changes.

Configuring Citrix Secure Gateway Support

In this example, you want to specify a Citrix Secure Gateway server called "csg1.citrix.com", on which ICA Clients use port 443, using the following two Secure Ticket Authority addresses:

- `http://server1.citrix.com/scripts/CtxSta.dll`
- `http://server2.citrix.com/scripts/CtxSta.dll`

Include the following six lines in NFuse.conf:

```
SessionField.NFuse_CSG_STA_URL1=http://server1.citrix.com/
scripts/CtxSta.dll
SessionField.NFuse_CSG_STA_URL2=http://server2.citrix.com/
scripts/CtxSta.dll
SessionField.NFuse_CSG_Server=csg1.citrix.com
SessionField.NFuse_CSG_ServerPort=443
SessionField.NFuse_CSG_Enable=On
SessionField.NFuse_CSG_AddressTranslation=normal
```

Restart the Web server to apply the changes.

Making NFuse Classic Available to Users

When NFuse Classic is installed and configured, inform your users of the URL for the NFuse Classic Login page. By default, the URL for the NFuse Classic 1.7 Login page is: `http://servername/Citrix/NFuse17`.

For NFuse Classic servers installed as part of MetaFrame XP, if you changed your default Web page during the installation, the default Web page for your MetaFrame server (`http://servername`) is the NFuse Classic Login page. Otherwise, the URL is: `http://servername/Citrix/NFuse17`.

Making the Login Page the Default Web Page

You can make the NFuse Classic Login page the default Web page for your MetaFrame server, so that users can point their browsers to `http://servername/` instead of `http://servername/Citrix/NFuse17/`.

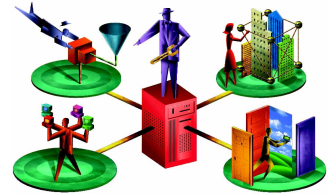
To do this, you create a `default.htm` page that redirects users from `wwwroot` to the `/Citrix/NFuse17` folder. You then save this page as `wwwroot\default.htm`. For example:

```
<HTML><HEAD>
<META HTTP-EQUIV="Refresh" CONTENT="0;URL=/Citrix/NFuse17/">
</HEAD></HTML>
```

What to Do Next

- For more information about deploying ICA Clients to your NFuse Classic users or about configuring the ICA Macintosh Client, see “ICA Clients and NFuse Classic” on page 109.
- For information about security considerations, see Chapter 5, “Configuring NFuse Classic Security” on page 117.

ICA Clients and NFuse Classic



Overview

This chapter provides information about deploying and using ICA Clients with NFuse Classic. It explains how to deploy ICA Clients to your users using the Web-based ICA Client installation feature, and provides additional information about the ICA Java Client. Topics include:

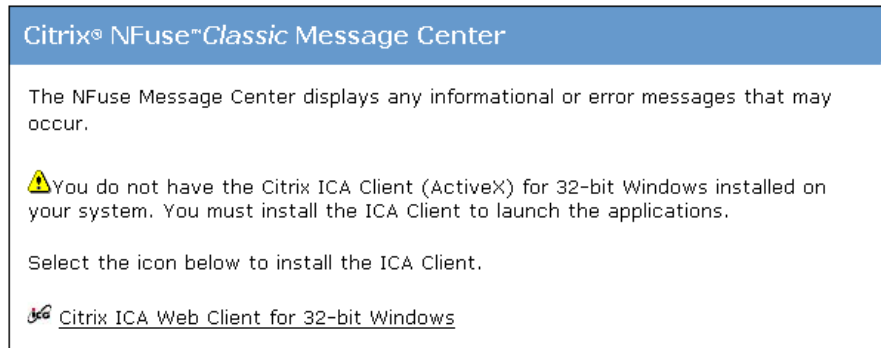
- Web-based ICA Client installation
- About the ICA Java Client
- The ICA Win32 Program Neighborhood Agent
- ICA Macintosh Client Web browser configuration

About Web-Based ICA Client Installation

To use NFuse Classic, users must have a supported Web browser and an ICA Client.

One method of deploying and installing ICA Clients on your users' devices is using Web-based ICA Client installation, which is a default component of NFuse Classic. This feature uses HTML documents and ICA Client installation files, stored on a Web server, to determine the type of client device and Web browser, and display the user with a link to the appropriate ICA Client installation file. When users click on a link, the ICA Client is installed on their client device. The links presented to users are called *installation captions*.

The following shows a typical installation caption:



Copying ICA Client Installation Files to your Web Server

To use Web-based ICA Client installation, your Web server must contain the ICA Client installation files.

During NFuse Classic installation, Setup prompts you to supply the Components CD-ROM 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 NFuse Classic Setup: `<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 NFuse Classic on a typical Internet Information Server Web server, the ICA Win32 Client is contained in the following directory: C:\inetpub\WWWRoot\Citrix\ICAWEB\en\ICA32.

If you did not copy the ICA Client installation files to your Web server during NFuse Classic installation, make sure you copy these 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 the Components CD-ROM in your Web server's CD-ROM drive or browse your network for a shared Components 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.

Configuring Web-Based ICA Client Installation

This section explains how to configure the installation captions presented to users, and the ICA Win32 Client offered to Windows client devices. It explains how to do this using the NFuse.conf file.

Note For information about configuring Web-based ICA Client installation using the Admin tool, see “Configuring Web-Based ICA Client Installation” on page 83.

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. However, you can modify this behavior so that the ICA Win32 Program Neighborhood Client or the Program Neighborhood Agent are offered instead.

The following describes the differences between these installation files:

- **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 and Ica32.msi).** Installs all components of the ICA Win32 Client including the Program Neighborhood user interface. You must use the Ica32.exe or Ica32.msi archive to install the ICA Win32 Client if your users require full ICA Client functionality.

- **ICA Win32 Program Neighborhood Agent installation file (Ica32a.exe and Ica32a.msi).** Installs all components of the ICA Win32 Client including the Program Neighborhood Agent user interface. You can use Ica32a.exe or Ica32a.msi to allow users to access NFuse Classic-enabled published applications directly from the Windows desktop, Start menu, or in the Windows System Tray.

► **To configure NFuse Classic to offer a different ICA Win32 Client**

1. Open the NFuse.conf file.
2. Edit the **Win32Client** parameter. For example:

```
Win32Client=Click here for the Client&/Citrix/ICAWEB/en/ica32/ica32.exe
```
3. Restart the Web server to apply your changes.

Configuring Installation Captions

You can configure whether or not installation captions are presented to users and the text displayed in the captions. To do this you use the **ShowClientInstallCaption** and **OverrideClientInstallCaption** parameters in NFuse.conf.

Note For information about configuring installation captions using the Admin tool, see “Configuring Web-Based ICA Client Installation” on page 83.

The **ShowClientInstallCaption** parameter specifies whether or not Web-based ICA Client installation captions are displayed to users. There are three options:

- **auto**—on Windows platforms, if the user does not have an ICA Client installed, an installation caption is displayed. On other platforms, the installation caption is always shown. This is the default setting.
- **on**—the installation caption is always displayed on all platforms.
- **off**—the installation caption is never displayed.

The **OverrideClientInstallCaption** parameter specifies a custom message that can 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:

“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. Select the icon below to install the ICA Client.”

► **To display a custom message with the download links**

1. Open the NFuse.conf file.
2. Edit the **OverrideClientInstallCaption** parameter. For example:

```
OverrideClientInstallCaption=Please install an ICA Client. Here  
are the clients we offer:
```
3. Restart the Web server to apply your changes.

About the ICA Java Client

If you are deploying ICA Clients over a low-bandwidth network or you are not sure what platform your users are on, consider using the ICA Java Client. The ICA Java Client is a Java applet that is cross-platform compatible and can be deployed by the NFuse Classic server to any Java-compatible Web browser.

Using NFuse Classic, you can configure the ICA Java Client to be a small download (as small as 300K) by removing unwanted components. Alternatively, you can configure NFuse Classic to allow users to control which ICA Java Client components they require. For more information about how to configure the components included in the deployment of the Java Client using the Admin tool, see “Customizing ICA Java Client Deployment” on page 87.

The ICA Java Client is optimized for zero-residence download-and-run deployment, where it is not possible or desirable to install an ICA Client on the client device.

You can also deploy the ICA Java Client independently of NFuse Classic. For more information, see the *Citrix ICA Java Client Administrator's Guide*.

New in version 6.3 of the ICA Java Client is the ability for the user to adjust client settings using a graphical user interface, when the ICA Java Client is running as an applet. See the *Citrix ICA Java Client Administrator's Guide* for more information.

About the ICA Win32 Program Neighborhood Agent

The ICA Win32 Program Neighborhood Agent allows you to seamlessly integrate published content with users' desktops. With the Program Neighborhood Agent, users can access remote applications by clicking icons on the Windows desktop, in the Start menu, in the Windows system tray, or a combination of these.

The Program Neighborhood Agent operates in the background. It has no user interface, except for a shortcut menu in the system tray. Therefore, working with remote applications has the look and feel of working with local applications.

The default properties for all Program Neighborhood Agents on your network are controlled by a single, editable configuration file called **Config.xml**. This file is placed on the NFuse Classic server during NFuse Classic installation. You can edit Config.xml to dynamically manage and control the clients on your network. For example, you can edit Config.xml to prevent users from editing certain settings and to "push" specific Program Neighborhood Agent settings to the client device.

Client/server data transfer occurs over standard HTTP or HTTPS protocols, which makes it easy to use the Program Neighborhood Agent in conjunction with firewalls using port 80.

For information about installing and configuring the Program Neighborhood Agent, see the *ICA Win32 Clients Administrator's Guide*.

Configuring the ICA Macintosh Client

Most ICA Clients require no configuration after installation to work with NFuse Classic; however, for clients using NFuse Classic on a Macintosh with Netscape Navigator, further configuration is required. No configuration is required on a Macintosh for Internet Explorer Version 5.

This section provides instructions for configuring the browser on a Macintosh to associate the ICA Macintosh Client with the application/x-ica MIME type.

Registering Application/x-ica as a MIME Type

To configure the ICA Macintosh Client, you must manually register application/x-ica as a MIME type in the client device's browser. 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

Note The following instructions describe how to configure Netscape Navigator Version 6.01 for use with the ICA Macintosh Client. For 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 **Helper Applications**.
 4. Click **New Type**. The **New Type** dialog box is displayed.
 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, either type in the location or click **Choose** to browse to the location of the Citrix ICA Connection Center.
9. Click **OK**.

What to Do Next

For information about security considerations, see Chapter 5, “Configuring NFuse Classic Security” on page 117.

Configuring NFuse Classic Security



Overview

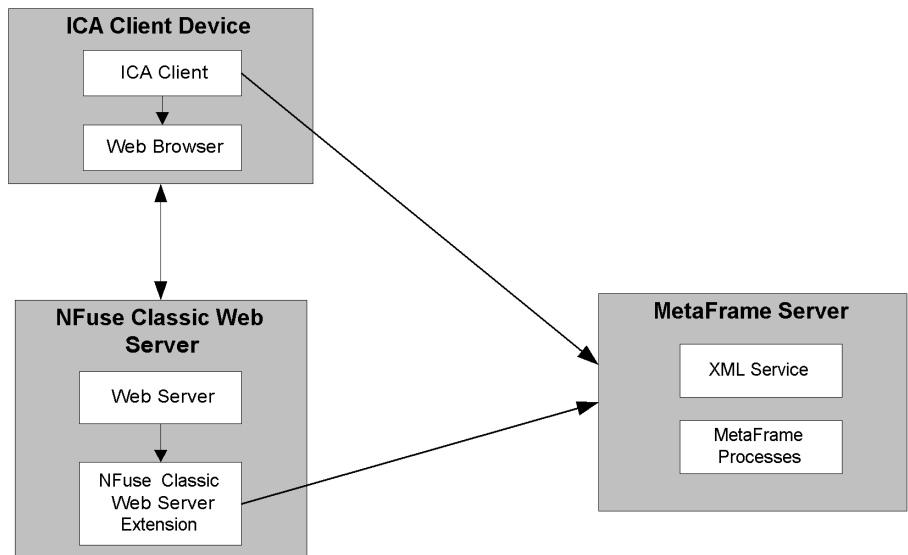
This chapter provides information about how to secure your data in an NFuse Classic environment. Topics include:

- Introduction to NFuse Classic security considerations and solutions
- Security between the ICA Client Device and NFuse Classic Server
- Security between the NFuse Classic Server and MetaFrame Server
- Security between the ICA Client Device and MetaFrame Server
- General security considerations

Introduction

A comprehensive security plan must include the protection of your data at all points in the application delivery process. This chapter describes NFuse Classic security risks and recommendations for each of the following communication links:

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



About Security Protocols and Citrix Security Solutions

This section introduces some of the security protocols and Citrix solutions you can use to secure your NFuse Classic deployment. It provides introductory information about the SSL and TLS security protocols, Citrix SSL Relay, Citrix Secure Gateway, and ICA Encryption. It also tells you where to find more information about these technologies.

SSL

The SSL (Secure Sockets Layer) protocol provides the ability to secure data communications across networks. SSL provides server authentication, encryption of the data stream, and message integrity checks.

SSL uses cryptography to encode messages, authenticate their identity, and ensure the integrity of their contents. This guards against risks such as eavesdropping, misrouting, and data manipulation. SSL relies on public key certificates, issued by certificate authorities, to ensure proof of identity.

For more information about SSL, cryptography, and certificates, see the *Citrix MetaFrame Administrator's Guide*, the *Citrix SSL Relay for UNIX Administrator's Guide* and the *Citrix Secure Gateway Administrator's Guide*.

TLS

TLS (Transport Layer Security) is the latest, standardized version of the SSL protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when they took over responsibility for the development of SSL as an open standard. Like SSL, TLS provides server authentication, encryption of the data stream, and message integrity checks.

Support for TLS Version 1.0 is included in Feature Release 2 for MetaFrame XP. Because there are only minor technical differences between SSL Version 3.0 and TLS Version 1.0, the server certificates you use for SSL in your MetaFrame installation will also work for TLS.

Some organizations, including US government organizations, require the use of TLS to secure data communications. These organizations may also require the use of validated cryptography, such as FIPS140. FIPS (Federal Information Processing Standard) is a standard for cryptography.

Note The maximum SSL/TLS certificate key size supported by NFuse Classic is 2048 bits.

Citrix SSL Relay

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

SSL Relay operates as an intermediary in the communication between the NFuse Classic server and Citrix XML service. When using 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 then sends all information requests in encrypted form to SSL Relay. SSL Relay decrypts the requests and passes them to the Citrix XML service. When returning the information to the Web server, the MetaFrame 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.

For more information about Citrix SSL Relay, see the *Citrix MetaFrame Administrator's Guide* or the *Citrix SSL Relay for UNIX Administrator's Guide*.

ICA Encryption (Citrix SecureICA)

Using ICA Encryption (Citrix SecureICA), you can encrypt the information sent between a MetaFrame server and an ICA Client. This makes it virtually impossible for unauthorized users to open an encrypted transmission and, in the unlikely event that an attack succeeds, ICA Encryption ensures that the attacker sees only meaningless screen commands and not sensitive information.

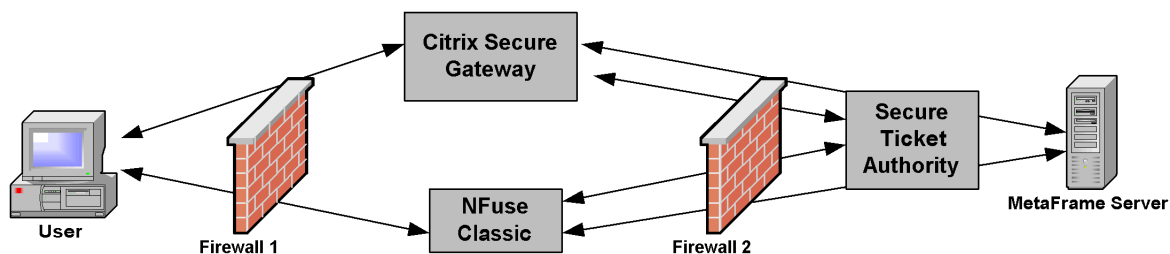
Therefore, ICA Encryption provides confidentiality to guard against the threat of eavesdropping. However, there are other security risks and using encryption is only one aspect of a comprehensive security policy. Unlike SSL/TLS, ICA Encryption does not provide authentication of the MetaFrame server. Therefore information could, in theory, be intercepted as it crosses the network and re-routed to a counterfeit server. Also, ICA Encryption does not provide integrity checking.

ICA Encryption is not available for MetaFrame for UNIX Operating Systems servers.

Citrix Secure Gateway

You can use Citrix Secure Gateway with NFuse Classic to provide a single, secure, encrypted point of access through the Internet to MetaFrame servers on your internal corporate networks.

Citrix Secure Gateway acts as a secure Internet gateway between SSL/TLS-enabled ICA Clients and MetaFrame XP servers. The Internet portion of ICA traffic between client devices and the Citrix Secure Gateway server is encrypted using SSL/TLS. This means that users can access information remotely without compromising security. Citrix Secure Gateway also simplifies certificate management, because you require a certificate only on the Citrix Secure Gateway server, rather than on every MetaFrame server in the farm.



For more information about Citrix Secure Gateway, see the *Citrix Secure Gateway Administrator's Guide*. For information about how to configure NFuse Classic for Citrix Secure Gateway support using the Admin tool, see "Configuring Citrix Secure Gateway Support" on page 74.

ICA Client Device—NFuse Classic Server Communication

Communication between ICA Client devices and the NFuse Classic server consists of passing several different types of data. As users identify themselves, browse applications, and eventually select 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 Classic 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 Classic form passes the user name as clear text and uses only basic encryption for the domain name and password.
- **HTML pages and session cookies.** After the user enters credentials in the NFuse Classic Login page, the user's credentials are stored on the Web server and protected by a session cookie. 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 (except in the case of smart card authentication).

Risks

Attackers can exploit NFuse Classic 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 session cookie, and HTML pages in transit between the Web server and Web browser.
- Although the session cookie used by NFuse Classic 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 use credential information.
- Although the ICA file does not contain any user credentials, it contains a one-time use ticket that expires in 200 seconds, by default. An attacker may be able to use the intercepted ICA file to connect to the MetaFrame server before the authorized user can use the ticket and make the connection.
- If the pass-through authentication feature is enabled on the Win32 ICA Client, an attacker could send the user an ICA file that causes the user's credentials to be misrouted to an unauthorized or counterfeit MetaFrame server.

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/TLS-Capable Web Servers and Web Browsers

Securing the Web server to Web browser component of NFuse Classic communication begins with implementing secure Web servers and Web browsers. Many secure Web servers rely upon SSL/TLS 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, TLS (Transport Layer Security) or Secure Socket Layer (SSL) message integrity checks ensure that the data has not been tampered with in transit.

In an NFuse Classic deployment, SSL/TLS authentication and encryption creates a secure connection over which the user can pass credentials posted in the NFuse Classic 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/TLS technology on your network, you must have a SSL/TLS-capable Web server and SSL/TLS-capable Web browsers. The use of these products is transparent to NFuse Classic. Configuration of your Web servers or browsers for NFuse Classic is not needed. For information about configuring your Web server to support SSL/TLS, see your Web server's documentation.

Important Many SSL/TLS-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 MetaFrame server running the SSL Relay, make sure you configure either the Web server or SSL Relay to use a different port.

Do Not Enable Pass-through Authentication

To prevent the possible misrouting of user credentials to an unauthorized or counterfeit MetaFrame server, do not enable the pass-through authentication feature in a secure installation. Use this feature only in a small, trusted environment.

NFuse Classic Server—MetaFrame Server Communication

Communication between the Web server and MetaFrame server in an NFuse Classic deployment involves passing user credential and application set information between the NFuse Classic Java objects on the Web server and the Citrix XML Service in the server farm.

In a typical NFuse Classic 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 obfuscation. 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 the obfuscation can obtain user credentials as well.
- An attacker can impersonate the MetaFrame 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 server farm:

- Use Citrix SSL Relay as a security intermediary between the Web server and server farm. Citrix SSL Relay performs host authentication and data encryption.
- In deployments that do not support running the SSL Relay, run the NFuse Classic server on your MetaFrame server.
- Use the HTTPS protocol to send the NFuse Classic data over a secure HTTP connection using SSL.

Use Citrix SSL Relay

Citrix 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 a Feature Release 1 license installed and activated.

On the MetaFrame server side, you must install a server certificate on the SSL Relay server and verify 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. For MetaFrame for UNIX servers, see the *Citrix SSL Relay for UNIX Administrator's Guide*.

When configuring the SSL Relay, make sure your SSL Relay server permits passing SSL traffic to the MetaFrame 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 Classic data, make sure the SSL Relay's server list contains the server to which you want to forward NFuse Classic data.

You can configure NFuse Classic to use Citrix SSL Relay using the Admin tool or the NFuse.conf file. For information about using the Admin tool, see "Configuring Communication With MetaFrame" on page 49.

► **To configure NFuse Classic to use Citrix SSL Relay using NFuse.conf**

1. Open the NFuse.conf file.
2. Change **SessionField.NFuse_RelayServerPort** to the port number of the SSL Relay on the server.
3. Change the value of **SessionField.NFuse_Transport** to **SSL**.
4. Restart the Web server to apply your changes.

Tip For an example of how to configure NFuse Classic to use Citrix SSL Relay using NFuse.conf, see "Configuring SSL Relay Communication" on page 105.

Adding Certificates to the NFuse Classic Server

NFuse Classic 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 NFuse Classic Server.

► **To add a new root certificate to your NFuse Classic server**

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*. For MetaFrame for UNIX servers, see the *SSL Relay for UNIX Administrator's Guide*.

Run the NFuse Classic Server on Your MetaFrame Server

For those deployments that do not support SSL Relay, you can eliminate the possibility of network attack by running a Web server on the MetaFrame server supplying the NFuse Classic data. Hosting your NFuse Classic Web sites on such a Web server routes all NFuse Classic requests to the Citrix XML Service on the local host, thereby eliminating transmission of NFuse Classic data across the network.

However, the benefit of eliminating network transmission must be weighed against the risk of exploitation of the Web server. Note also that if there are multiple MetaFrame servers in the farm, credentials will still be passed in clear text between MetaFrame servers when NFuse acquires a MetaFrame ticket.

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 enable 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 MetaFrame 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 MetaFrame 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 MetaFrame 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 Classic with network address translation, see “Setting NFuse Server Location Options” in the *Customizing NFuse Classic guide*. This topic includes information about server location through firewalls.

Use the HTTPS Protocol

You can use the HTTPS protocol to secure the NFuse Classic data passing between the Web server and MetaFrame server. HTTPS uses SSL/TLS to provide strong encryption of data.

The Web server makes an HTTPS connection to IIS running on the MetaFrame server. This requires IIS port sharing at the MetaFrame server, and for IIS running on the MetaFrame server to have SSL enabled. The server name you specify (using the Admin tool, or in **SessionField.NFuse_CitrixServer** in *NFuse.conf*) must be a fully-qualified DNS name that matches the name of the IIS SSL server certificate. The XML service is reached at: `https://NFuse_CitrixServer/scripts/wpnbr.dll`.

For information about how to configure NFuse Classic to use the HTTPS protocol using the Admin tool, see “Specifying the Transport Protocol” on page 52.

► To configure NFuse Classic to use HTTPS using the *NFuse.conf* file

1. Open the *NFuse.conf* file.
2. Change **SessionField.NFuse_Transport** to **HTTPS**.
3. Restart the Web server to apply your changes.

ICA Client—MetaFrame Server Communication

NFuse Classic communication between client devices and MetaFrame 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. These parameters control various aspects of the ICA session such as which 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 MetaFrame server as the user navigates the chosen application. In response, the MetaFrame server sends the ICA Client graphical updates.

Risks

To capture and interpret ICA Client to MetaFrame 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 MetaFrame server.

Recommendations

Use SSL/TLS or ICA Encryption

Citrix recommends implementing SSL/TLS or ICA Encryption to secure the traffic between your ICA Clients and MetaFrame servers. Both methods support 128-bit encryption of the data stream between the ICA Client and MetaFrame server, but SSL/TLS 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 SSL/TLS is included in Feature Release 2 for MetaFrame XP. Support for ICA Encryption is included in Feature Release 1 for MetaFrame 1.8 and MetaFrame XP.

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 about ICA Encryption.

Use Citrix Secure Gateway

You can use Citrix Secure Gateway to secure the traffic between your ICA Clients and MetaFrame servers over the Internet. Citrix Secure Gateway acts as a secure Internet gateway between SSL/TLS-enabled ICA Clients and MetaFrame XP servers.

For more information about Citrix Secure Gateway, see the *Citrix Secure Gateway Administrator's Guide*. For information about how to configure NFuse Classic for Citrix Secure Gateway support using the Admin tool, see “Configuring Citrix Secure Gateway Support” on page 74.

General Security Considerations

Citrix recommends that, as with any Windows-based server, you follow Microsoft standard guidelines for configuring your Windows server. In particular, when you install the server, do not use a FAT (File Allocation Table) file system, because this may allow users other than administrators to run the NFuse Classic Admin tool.

Always ensure your Microsoft Internet Information Server (IIS) is up to date with all the latest patches. See Microsoft's Web site for details.

Index

A

- Active Server Pages 12
- address translation
 - and Citrix Secure Gateway 75, 101
 - configuring 66, 95
 - examples of how to configure 70
- Admin tool
 - about 15, 46
 - accessing 47
 - configuring NFuse Classic with 47–90
- alternate address
 - and Enterprise Services mode 89
 - configuring 67–68, 93
- application publishing 18
- application set 18
- applying changes 48, 91
- appsrv.ini file
 - editing for Single Sign On 58
 - editing for smart card support 61
- authentication
 - configuring 53–65, 94
 - recommendations 54
- automatic deployment of ICA Win32 Web Client
 - and Enterprise Services mode 89
 - configuring 84, 94

B

- backward compatibility 26

C

- certificate key size 119
- ciphersuite
 - configuring preferences 99
- Citrix Enterprise Services for NFuse
 - about 14, 89
 - considerations when upgrading 32
 - files installed 33
 - mode setting 89, 98

- Citrix NFuse Classic
 - configuring 46–106
 - features 13–17
 - how it works 20
 - installing 30–38
 - introduction to 12
 - making available to users 107
 - MetaFrame and ICA Client requirements for 25
 - running on a MetaFrame server 126
 - uninstalling 43
 - upgrading 31
 - user configuration of 80
 - user settings 92
- Citrix on the World Wide Web 11
- Citrix Secure Gateway
 - about 14, 121
 - between clients and MetaFrame 129
 - configuring NFuse Classic for 68–69, 74, 101
 - example of how to configure 76, 106
 - ticketing 74
- Citrix SSL Relay
 - configuring NFuse Classic for 52, 102, 105
 - overview 120
 - see also SSL
- Citrix XML Service
 - configuring communication with 49, 101, 105
 - configuring fault tolerance 50, 94
 - for UNIX Operating Systems 24
 - role in NFuse Classic 18
 - TCP/IP port configuration 51, 101
 - viewing the port assignment 34
- Components CD-ROM 28
- configuration file. See NFuse.conf
- Config.xml 114
- content publishing 14
 - enhanced 17
- context name 55
- context-sensitive help 48
- conventions, in the documentation 8
- cookies 81, 122

D

- default Web page, setting 107

Desktop Credential Pass-Through
 about 16, 53
 configuring 57, 94
 example of how to configure 63
documentation
 comments and suggestions 10
 conventions 8
 other sources 9
 using PDF 10
DTD file 95

E

embedding applications 16, 85, 92, 95
 and Enterprise Services mode 89
enhanced content publishing 17
Enterprise Services mode. See Citrix Enterprise Services
expiry time, of tickets 63
explicit authentication 53, 55

F

fault tolerance, configuring 50, 76, 94
File Allocation Tables (FAT) 129
firewall 126
 and Enterprise Services mode 89
 configuring address translation 66, 95
 configuring client-side settings 77

G

guest authentication 53, 56
 security considerations 57

H

help, displaying context-sensitive 48
HTTP 52, 102
HTTPS 52, 102, 127

I

ICA Client deployment. See Web-based ICA Client
 installation
ICA Client device
 requirements 28
 role in NFuse Classic 19
 security 122, 128
ICA Client files
 copying to your Web server 110
ICA Encryption 120, 128
ICA files 21, 122

ICA Java Client
 and embedded applications 86
 and Enterprise Services mode 89
 deployment of components 82, 87, 97
 overview 113
ICA Macintosh Client
 configuring for NFuse Classic 115
ICA session
 user configuration of 80
 user settings 92
ICA Win32 Client 104
 about the different files 111
 configuring for Single Sign On 58
 configuring for smart card support 60
 ICA Win32 Program Neighborhood Agent 15, 114
 ICA Win32 Web Client
 automatic deployment of 82, 84, 94
icon files 38, 102
IISRESET command 91
IIS. See Internet Information Server
initialization 128
installation captions 83, 95, 102, 104, 110, 112
 overriding 99
installing NFuse Classic
 on IIS 35
 on UNIX platforms 36
 overview 30
 security considerations 33
Internet Information Server
 requirements 27
 security considerations 129
 stopping and restarting 91
IP address prefix. See partial IP address
iPlanet
 configuring the Web server 39
 installing NFuse Classic on 36
 uninstalling on 44
ISAPI 13

J

Java Client. See ICA Java Client
Java objects 12, 19, 21, 31–32, 37, 42
Java Virtual Machine 27
JavaServer Pages 12, 46
JVM. See Java Virtual Machine

L

- load balancing
 - and Enterprise Services mode 89
 - between Secure Ticket Authorities 75, 96
 - XML requests 16, 51, 96
- Login page 53, 56, 107

M

- MetaFrame for UNIX Operating Systems
 - configuration requirements 26
 - determining XML Service port 34
 - requirements 24
 - role in NFuse Classic 18
 - support 14
- MetaFrame server
 - configuring communication with 49, 101, 105
 - requirements 24
 - role in NFuse Classic 18
 - security considerations 124, 128
- Microsoft domain-based authentication 55, 96, 98

N

- NAT. See network address translation
- NDS
 - authentication 25, 55, 98, 100
 - support 13
- Netscape Navigator
 - supported versions 29
 - using with the ICA Macintosh Client 115
- network address translation 16, 66, 95
 - and Citrix Secure Gateway 75, 101
 - examples of how to configure 70
- NFuse
 - see Citrix NFuse Classic
- NFuse.conf 31, 46
 - configuring NFuse Classic with 91–104
 - location of 32, 37
- NT authentication 55, 96, 98
- NTLM. See Desktop Credential Pass-through

O

- online help 48
- overview of NFuse Classic 20

P

- partial IP address 68, 95

- pass-through authentication 16, 54, 99
 - and smart card support 63
 - combining with Desktop Credential Pass-through 59
 - example of how to configure 63
 - security considerations 58, 123
- password
 - enabling users to change 16, 55, 93
 - for Enterprise Services mode 90, 98
- PDF, using 10
- port address translation 67
 - example of how to configure 72
- protocol, transport 52, 102

R

- readme file 9
- registering application/x-ica 115
- repair option 42
- root certificates, adding 126

S

- Secure Sockets Layer. See SSL
- Secure Ticket Authority 74, 101
- secure Web servers 123
- SecureICA. See ICA Encryption
- security 117–129
 - and guest authentication 57
 - Citrix Secure Gateway 121
 - between clients and MetaFrame 129
 - configuring NFuse Classic for 74
 - general considerations 129
 - ICA Encryption 120
 - network communication
 - between client device and NFuse Classic server 122
 - between ICA Client and MetaFrame server 128
 - between NFuse Classic server and MetaFrame

- server 124

- pass-through authentication 58, 123

- protocols and Citrix solutions 119

- SSL

- adding certificates 125

- between clients and MetaFrame 128

- between Web server and Web browser 123

- configuring the SSL Relay 124

- see also Citrix SSL Relay

- TLS

- between clients and MetaFrame 128

- between Web server and Web browser 123

- overview 119

- when installing NFuse Classic 33

- Single Sign On. See Desktop Credential Pass-Through

- smart card

- about 16, 54

- enabling authentication 60, 103

- example of how to configure 64

- requirements 60

- socket pooling 99

- SOCKS proxy server 16, 77

- configuring communication with 77, 103

- example of how to configure 79

- software directory 32, 91

- SSL

- adding certificates 125

- and ciphersuites 99

- and Citrix Secure Gateway 74

- between clients and MetaFrame 128

- certificate key size 119

- configuring the SSL Relay 124

- finding more information on the SSL Relay 9

- overview 119

- secure Web servers 123

- substitution tags 12, 46

- system requirements 24–29

- ICA Client device 28

- MetaFrame 24

- Web server 27

T

- ticketing 15, 122

- and Citrix Secure Gateway 74

- configuring ticket expiry time 63, 102

- TLS

- and ciphersuites 99

- and Citrix Secure Gateway 74

- between clients and MetaFrame 128

- certificate key size 119

- overview 119

- secure Web servers 123

- Tomcat

- installing NFuse Classic on 36

- uninstalling on 44

- translated address, configuring 67–69, 100

- Transport Layer Security. See TLS

- transport protocol 52, 102

- troubleshooting

- alternate address 89

- embedded applications 89

- firewall support 89

- load balancing 89

- MetaFrame 1.8 environments 26

- NFuse Classic installation 42

U

- uninstalling NFuse Classic 43

- UNIX platforms

- configuring the Web server for 39

- installing NFuse Classic on 36

- uninstalling on 43

- upgrading NFuse Classic 31

- UPN support 13, 61, 96

W

- Web pages 37

- setting the default 107

- Web server

- files copied to 37

- requirements 27

- role in NFuse Classic 19

- scripts 46

- security 123

- Web site, Citrix 11

- Web-based ICA Client installation 15, 19, 83, 110

- copying ICA Clients to your Web server 110

- WebSphere

- configuring the Web server 39

- installing NFuse Classic on 36

- uninstalling on 44

- Windows Directory Service Mapper 61

- Windows installer 13