
Configuring SSL Relay for NFuse 1.5 and Windows NT/2000 Web Servers

By Citrix Consulting Services

Citrix Systems, Inc.



CITRIX

Notice

The information in this publication is subject to change without notice.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

This publication contains information protected by copyright. Except for internal distribution, no part of this publication may be photocopied or reproduced in any form without prior written consent from Citrix.

The exclusive warranty for Citrix products, if any, is stated in the product documentation accompanying such products. Citrix does not warrant products other than its own.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Copyright © 2001 Citrix Systems, Inc., 6400 NW 6th Way, Ft. Lauderdale, Florida 33309 U.S.A. All rights reserved.

Version History		
February 9, 2000	Katherine Schaefer	Version 1.0



Table of Contents

OVERVIEW	1
CONFIGURING YOUR SERVERS	2
WEB SERVER CONFIGURATION	2
METAFRAME SSL RELAY SERVER CONFIGURATION	3
CREATING NFUSE WEB PAGES	5
CREATING A CERTIFICATE REQUEST USING IIS KEY MANAGER.....	6
WINDOWS NT	6
WINDOWS 2000.....	6
TROUBLESHOOTING TIPS.....	8
CERTIFICATE AUTHORITY SOURCES	9



Overview

This white paper explains how to install and configure SSL Relay for NFuse 1.5 and Windows NT/Windows 2000 Web servers.

Configuring your servers

Before enabling SSL Relay, you must first configure the Web server and the MetaFrame SSL Relay server.

The following servers are required to implement SSL Relay:

- A Web server with NFuse Web Extensions and Web Site Wizard
- A MetaFrame 1.8 server (with SP2/FR1) that will act as the SSL Relay server (required for SSL Relay Configuration Tool)

Web server configuration

Complete the following steps to configure the Web server.

1. Add the following information to the NFuse.properties file located in %SystemRoot%\java\trustlib on the Web server (see Figure 1 for an example):

```
NFuse_Transport=SSL
NFuse_RelayServer=fully-qualified domain name of SSL relay server
NFuse_RelayServerPort=port # (default is 443)
SSLKeyStore=path to cacert (this may already be included in the file)
```

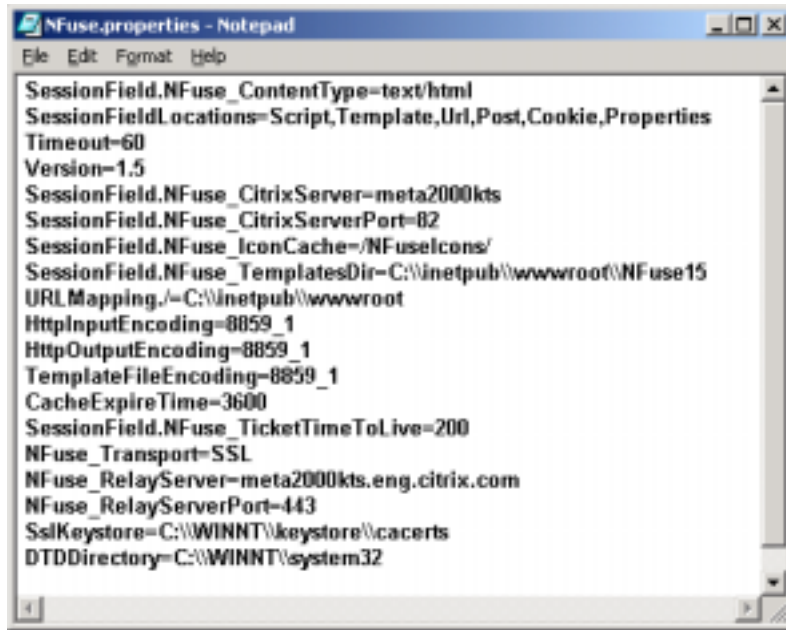


Figure 1

2. Obtain a signed certificate from a Certificate Authority and integrate the certificate with NFuse 1.5. See “Creating a Certificate Request Using IIS Key Manager” in this document for more information.

MetaFrame SSL Relay server configuration

Complete the following steps to configure the MetaFrame SSL relay server.

1. Select **Citrix SSL Relay Configuration** from **Start > Program Files > MetaFrame Tools** on the MetaFrame server.
2. Verify the settings on the Relay Credentials tab (see Figure 2 below). The SSL Relay Configuration tool generates the Server Certificate field. The Server Certificate field derives the fully qualified domain name from the certificate located in the directory you specify in the Key Store Location field. The “certs” directory is not included in the Key Store Location field.

Enter the password created in IIS Key Manager (Windows NT 4.0) or Internet Services Manager (Windows 2000) for this server certificate.

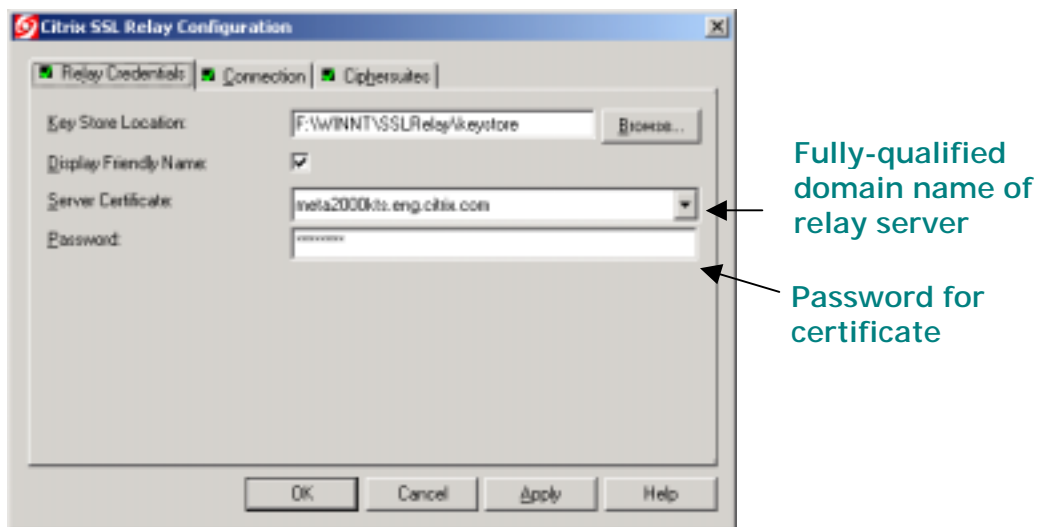


Figure 2

3. On the **Connection** tab, displayed in Figure 3 below, type the Relay Listening Port that was selected for the NFuse.properties file.

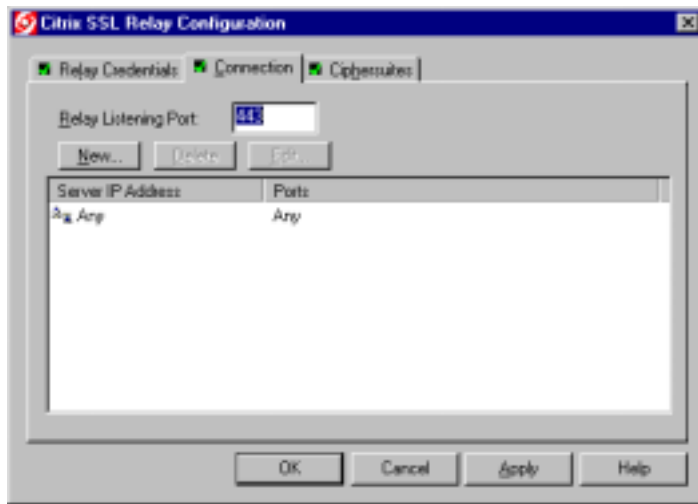


Figure 3

Click **New** and enter the IP Address(es) and Destination Port(s) for the MetaFrame server(s) that will receive XML data from the SSL Relay server. Click **OK**. [In Figure 3, "Any" was selected for the Server IP Address and Ports for simplification.]

Delete the old server IP address (if any) and click **OK**.

4. Click **OK** to exit the Citrix SSL Relay Configuration tool. Click **Yes** when prompted to start the Citrix SSL Relay Service.

Note: For debugging purposes, you can click **NO** in Step 4 and start the service from the command line. From the command line, go to %systemroot%\SSLRelay\SSLServerRelay.exe to start the service. You can verify that there were no errors when starting it and when connecting to the SSL server.

The service has started correctly when "Waiting for incoming connections" appears on the screen, as shown in Figure 4.

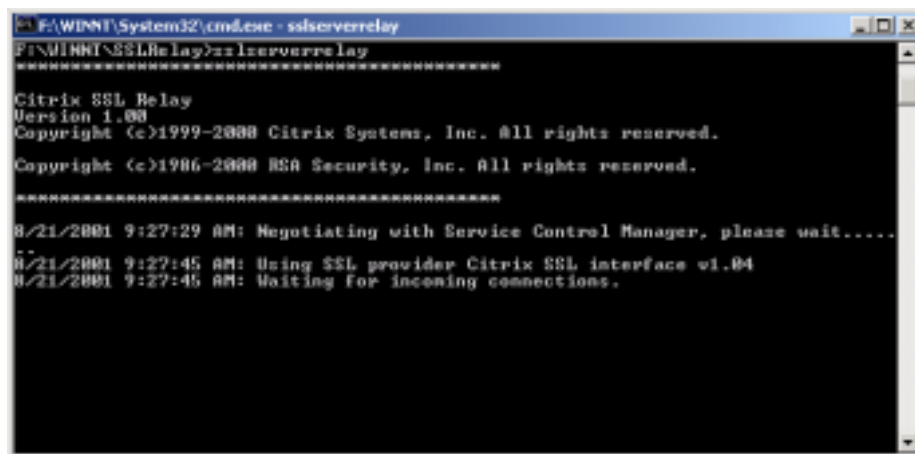
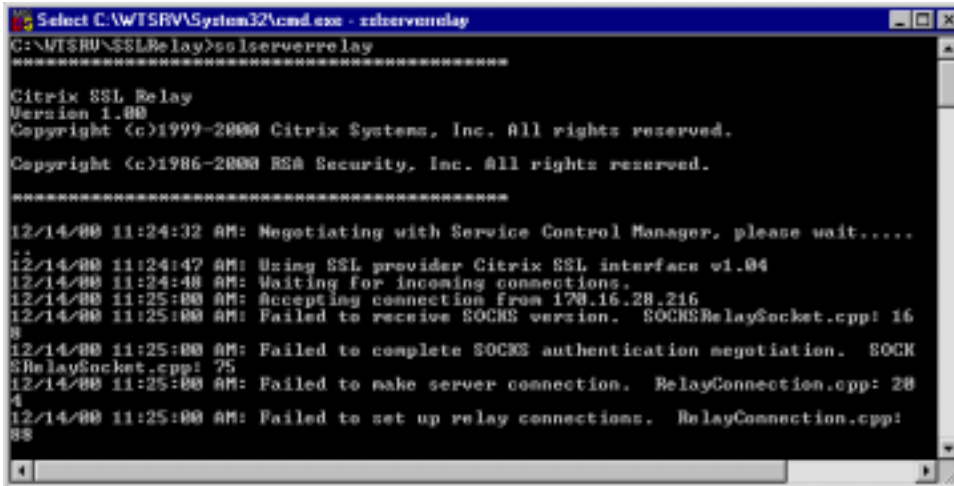


Figure 4

Creating NFuse Web pages

Use the Web Site Wizard to create template NFuse pages. When you are prompted to Enable SSL Relay, check the box and provide the fully qualified domain name and the port number of the SSL Relay. SSL is now enabled for use with NFuse.

Important: You must include the fully qualified domain name of the SSL Relay Server. The SSL Relay Service does not recognize the NetBIOS name of the server. If you enter the NetBIOS name, the error displayed below in Figure 5 is generated:



```
Select C:\WINDOWS\system32\cmd.exe - sslserverrelay
C:\NTSRV\SSLRelay>sslserverrelay
*****
Citrix SSL Relay
Version 1.00
Copyright (c)1999-2000 Citrix Systems, Inc. All rights reserved.
Copyright (c)1986-2000 RSA Security, Inc. All rights reserved.
*****

12/14/00 11:24:32 AM: Negotiating with Service Control Manager, please wait....
..
12/14/00 11:24:47 AM: Using SSL provider Citrix SSL interface v1.04
12/14/00 11:24:48 AM: Waiting for incoming connections.
12/14/00 11:25:00 AM: Accepting connection from 170.16.28.216
12/14/00 11:25:00 AM: Failed to receive SOCKS version. SOCKSRelaySocket.cpp: 16
#
12/14/00 11:25:00 AM: Failed to complete SOCKS authentication negotiation. SOCK
SRelaySocket.cpp: 75
12/14/00 11:25:00 AM: Failed to make server connection. RelayConnection.cpp: 28
#
12/14/00 11:25:00 AM: Failed to set up relay connections. RelayConnection.cpp:
88
##
```

Figure 5

Creating a Certificate Request Using IIS Key Manager

Windows NT

Complete the following steps to create a certificate request using IIS Key Manager on a Windows NT Web server:

On the Web server:

1. Open Internet Services Manager.
2. Click Default Web Site (or the Web site you configured for NFuse) and open the Properties window (or click the key button that appears on the tool bar).
3. On the Directory Security tab, click the **Key Manager** button.
4. Create a new key (certificate request). You must create a password for this key.
5. This password must also be entered into the Citrix SSL Relay Configuration tool. If you forget the password, you will need to create a new certificate.
6. Send this certificate request to a certificate authority. The certificate authority will give you a “signed” certificate.
7. Obtain the root certificate from the Certificate Authority and save it in the %SystemRoot%\keystore\cacerts file located on the Web server. Save the file as a .der file type.
8. Right-click the root certificate and select **Install Certificate** to register this Certificate Authority root certificate on your Web server.
9. Load the “signed” certificate back into IIS Key Manager by selecting **Install Key Certificate** from the Key menu.
10. Export the key/certificate pair by selecting **Export Key** from the Key menu. Save this on a disk as a .key file type.

On the MetaFrame SSL Relay Server:

1. Run the export from the steps above through the Keytopem.exe utility found in %SystemRoot%\SSLRelay. Drag the file (.key) onto the KeyToPem.exe. The resulting .pem file is saved to the same location where the .key file was saved.
2. Place the result (now converted to a .pem file) in the certs folder that the relay is configured to use (Located in %SystemRoot%\SSLRelay\keystore\certs on the SSL Relay server). This file must have the .pem extension to be recognized.

Windows 2000

Complete the following steps to create a certificate request using IIS key manager on a Windows 2000 Server:

On the Web server:

1. Open Internet Services Manager and right-click the Web site to be secured (the site you configured for use with NFuse).
2. Select **Properties**. Access the Directory Security tab. Click the **Server Certificate** button in the Secure Communications section.
3. The IIS Certificate Wizard starts. Select **Create a new certificate** and click **Next**.
4. Select the following options: Keep the default selection, Prepare the request now, but send it later.

5. Enter a name for the certificate and select the bit length. A certificate with a higher bit length has a more secure level of encryption.
6. Enter the organization name and organizational unit.
7. Enter the fully qualified domain name of the relay server when prompted for the Common Name.
8. Save the certificate and complete the remaining steps of the wizard.

Send this certificate request to a certificate authority. The certificate authority will give you a “signed” certificate. When you have received the signed certificate, complete the following steps.

Note: The following procedure was compiled using a test certificate obtained from the Certificate Authority at <http://www.thawte.com/>.

1. Obtain the root certificate from the Certificate Authority and save it in the %SystemRoot%\keystore\cacerts directory. Save the file as a .der type file.
2. Right-click the root certificate file and select **Install Certificate** to register this Certificate Authority root certificate on your Web server.
3. Open Internet Services Manager and select **Properties**. Access the Directory Security tab and click the **Server Certificate** button.
4. Select **Process the pending request and install the certificate**.
5. When prompted, enter the path where you saved the signed certificate. Complete the remaining steps of the wizard.
6. On the Directory Security tab, click **View Certificate**.
7. On the Details tab, click **Copy to File** to export the key/certificate pair. Complete the remaining steps of the wizard, accepting all default settings. When prompted, enter a password for the certificate. This password is used when configuring the SSL Relay Service.
8. You are prompted for a file name for export. Save the file to a location accessible to the SSL Relay Server. Rename the file with a .key extension (the export process saves it as a .pfx file).

On the MetaFrame SSL Relay Server:

1. Run the export from the steps above through the Keytopem.exe utility found in %SystemRoot%\SSLRelay. Drag the file (.key) onto the KeyToPem.exe. The resulting .pem file is saved to the same location where the .key file was saved.
2. Place the result (now converted to a .pem file) in the certs folder that the relay is configured to use (Located in %SystemRoot%\SSLRelay\keystore\certs on the SSL Relay server). This file must have the .pem extension to be recognized.

Troubleshooting tips

The following troubleshooting tips address errors you may encounter when attempting to configure SSL Relay:

- Make sure that Internet services using the SSL port (TCP port 443) are not running on the SSL Relay MetaFrame server. If these services are running, the SSL Relay Service will encounter a port conflict and be unable to start.
- If you modify the NFuse.properties file, the IIS Admin and Web services must be stopped and restarted.
- If you start the SSL Relay Service from the command prompt and get the wrong SOCKS version error, check your date on the Web server. If the certificate was generated in another time zone, you may need to move the date forward and try again.
- The SOCKS version error is also generated when the Web server .der file is saved to the wrong directory. Make sure that you saved it in the %SystemRoot%\keystore\cacerts folder on the Web server (and not in the %SystemRoot%\SSLRelay\keystore\cacerts folder).
- Start the SSL Relay Service from the command prompt rather than from the Citrix SSL Relay to check for errors before attempting to use SSL with NFuse. Using the command prompt also lists errors encountered while using NFuse.
- Make sure that the keytool utility is used on the key/certificate pair that you exported from the Key Manager. When using the Citrix SSL Relay Configuration tool, an "incorrect password" error might arise if the wrong file was converted to .pem.

Certificate Authority Sources

The Certificate Authority generates a certificate using the request file from the Web server. The Certificate Authority uses the Web server's certificate request to create a "signed" certificate.

Certificate Authorities provide the test certificate services. Click the links below for more information about test certificates:

Thawte: <https://www.thawte.com/cgi/server/test.exe>

Baltimore: http://www.baltimore.com/sureserver/test_cert.html

Verisign: <https://www.verisign.com>

In addition to the above sources, the following Web sites provides background information regarding SSL. Click the following links to access this information:

Netscape: <http://developer.netscape.com/tech/security/basics/index.html>

<http://home.netscape.com/security/techbriefs/ssl.html>

<http://welcome.to/ssl>



6400 NW 6th Way

Fort Lauderdale, FL 33309

954-267-3000

<http://www.citrix.com>



Copyright © 2001 Citrix Systems, Inc. All rights reserved. Citrix, WinFrame and ICA are registered trademarks, and MultiWin and MetaFrame are trademarks of Citrix Systems, Inc. All other products and services are trademarks or service marks of their respective companies. Technical specifications and availability are subject to change without prior notice.