Stunnel Implementation Guide

Public Health Information Network Messaging System (PHINMS)

Version 1.1

Prepared by:
U.S. Department of Health & Human Services

September 20, 2006

EXECUTIVE SUMMARY

Public health involves many organizations throughout the PHIN (Public Health Information Network), working together to protect and advance the public's health. These organizations need to use the internet to securely exchange sensitive data between varieties of different public health information systems. The exchange of data, also known as "messaging" is enabled through messages created using special file formats and a standard vocabulary. The exchange uses a common approach to security and encryption, methods for dealing with a variety of firewall, and internet protection schemes. The system provides a standard way for addressing and routing content, a standard and consistent way for information systems to confirm an exchange.

The PHINMS (Public Health Information Network Messaging System) is the software which makes this work. The system securely sends and receives sensitive data over the internet to the public health information systems.

The following document provides instructions for installing and configuring Stunnel to secure and encrypt the route between the IIS Server/Jakarta Internet Server Application Programming Interface (ISAPI) redirect connector and the PHINMS Receiver/Tomcat server.

REVISION HISTORY

VERSION #	IMPLEMENTER	DATE	EXPLANATION
1.0	Lawrence Loftley	Aug 11, 2006	Create S-Tunnel Implementation Guide.
1.0	Wendy Fama	Aug 11, 2006	Update S-Tunnel Implementation Guide.
1.1	Wendy Fama	Sep 6, 2006	Add One to One Mapping.
1.1	Wendy Fama	Sep 19, 2006	Add Architecture section.
1.1	Wendy Fama	Sep 20, 2006	Update based on training feedback.

TABLE OF CONTENTS

LIST OF FIGURES

ACRONYM LIST

CDC	Centers for Disease Control and Prevention
DN	Distinguished Name
IIS	Internet Information Server
IP	Internet Protocol
ISAPI	Internet Server Application Programming Interface
JSP	Java Server Pages
PHIN	Public Health Information Network
PHINMS	Public Health Information Network Messaging System
SSL	Secure Socket Layers

1.0 INTRODUCTION

The Centers for Disease Control and Prevention (CDC) Public Health Information Network Messaging System (PHINMS) Stunnel Implementation Guide will assist with the installation and configuration of the Stunnel program on a Windows platform. Documentation is continually updated. Ensure the most recent versions are referenced from the PHINMS website at www.cdc.gov/phin/phinms.

1.1 Architecture

Redirecting messages from a Microsoft Integrated Information Server (IIS) as a proxy over an SSL connection to a PHINMS receiver requires the following multiple products:

- IIS Server,
- Jakarta ISAPI plug-in,
- Stunnel,
- Tomcat application server, and
- PHINMS Receiver.

Each component requires proper configuration for PHINMS messages only needed if IIS is being used as a web server, and BEA Web Logic is not being used as an application server.

Stunnel is setup between the IIS and the PHINMS Receiver servers. The Jakarta ISAPI redirector is pointed directly to the AJP13 port on the PHINMS Receiver server. When a firewall exists between the IIS proxy and the PHINMS Receiver, the firewall's UDP Port 500 must be open as shown in Figure 1.1. More information on self-signed certificates can be found at www.stunnel.org.

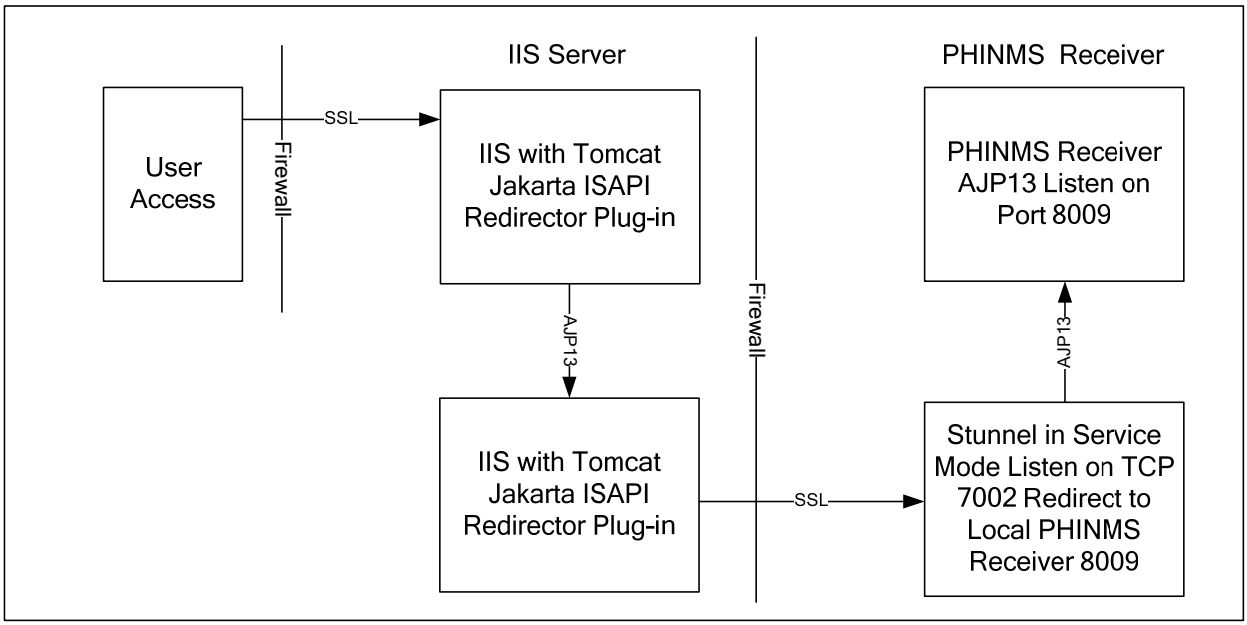

Figure 1.1. Stunnel Architecture Diagram

This Stunnel Implementation Guide is intended for those responsible for installing and configuring Stunnel and the Jakarta ISAPI to work with a PHINMS 2.6 receiver. It does not address installing or configuring the Tomcat application server nor PHINMS.

The information in this document has only been tested with the Tomcat application server. These settings may or may not work with other application servers such as JBOSS.

1.2 Stunnel

The Stunnel program is designed to work as a Secure Socket Layers (SSL) encryption wrapper between remote client and local or remote server. Stunnel can be used to add SSL functionality to commonly used servers without any changes in the programs' code.

1.3 Communiqués

The PHINMS team responds to user's communiqués. Send questions, suggestions, and/or comments concerning PHINMS support or documentation to the PHINMS website using the Contact PHINMS email link located at the top of the website.

2.0 STUNNEL CONFIGURATION

Implementing Stunnel based network communications between the Internet Information Server (IIS) Server and the PHINMS Receiver ensures all network communications between the two servers are encrypted and secure. Network traffic between the servers and other computers will not be affected by the installation of the Stunnel. Figure 2.1 shows the Stunnel architect.

2.1 Install Stunnel

Complete the following steps on both the IIS Server and the PHINMS Receiver to establish Stunnel between IIS and PHINMS Receiver:

1. navigate to http://www.stunnel.org/download/binaries.html displaying Figure 2.1,

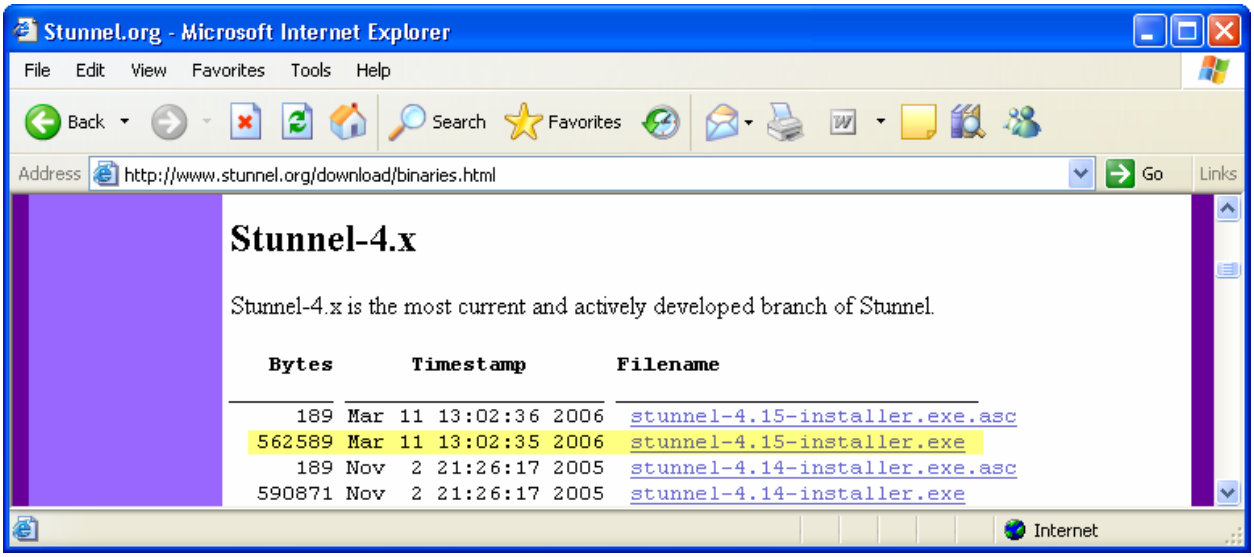

Figure 2.1. Stunnel-4.15-installer.exe

2. click **stunnel-4.15-installer.exe** link displaying the left screen of Figure 2.2, click **Run** displaying the right screen,

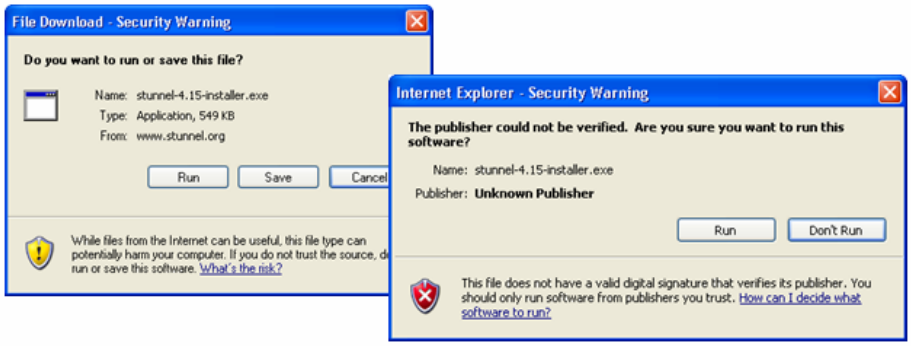

Figure 2.2. Stunnel Security Warning

3. click **Run** displaying Figure 2.3,

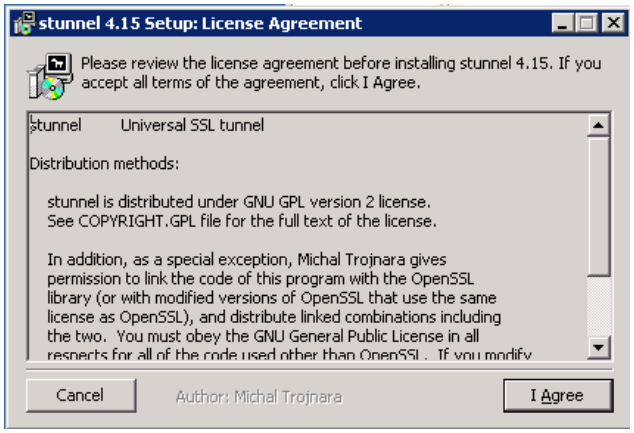

Figure 2.3. Stunnel License Agreement

4. read the **License Agreement**, select **I Agree** displaying Figure 2.4,

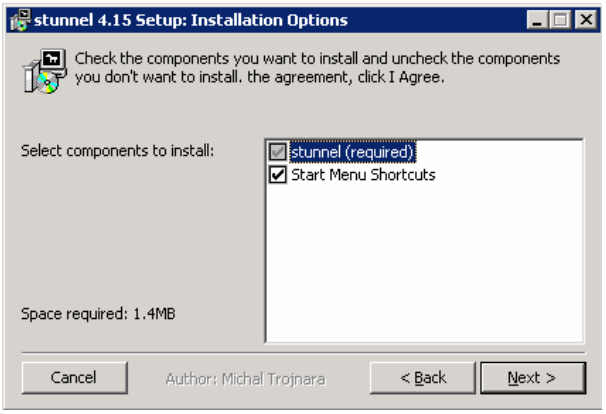

Figure 2.4. Stunnel Installation Options

5. check **Start Menu Shortcuts** (optional), select **Next** displaying Figure 2.5,

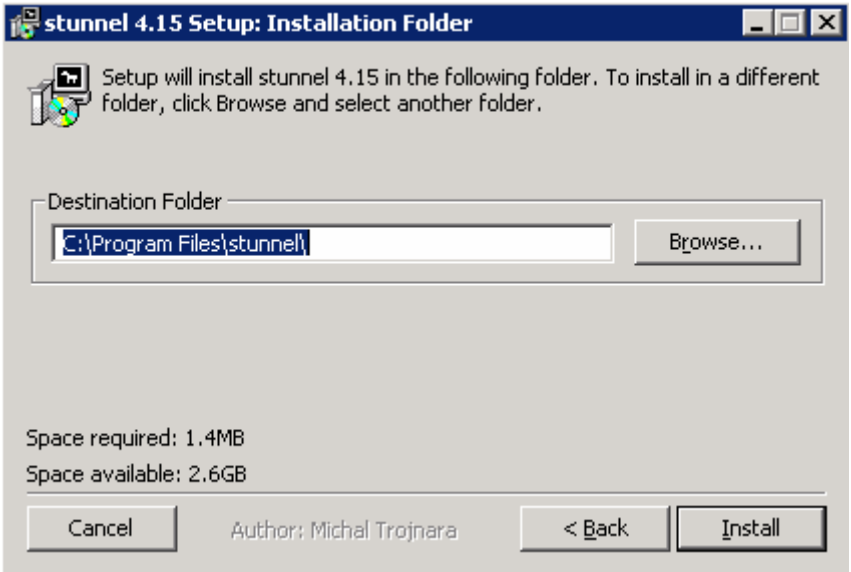

Figure 2.5. Stunnel Installation Folder

6. select **Browse** to choose a Destination Folder (optional), select **Install** displaying Figure 2.6, and

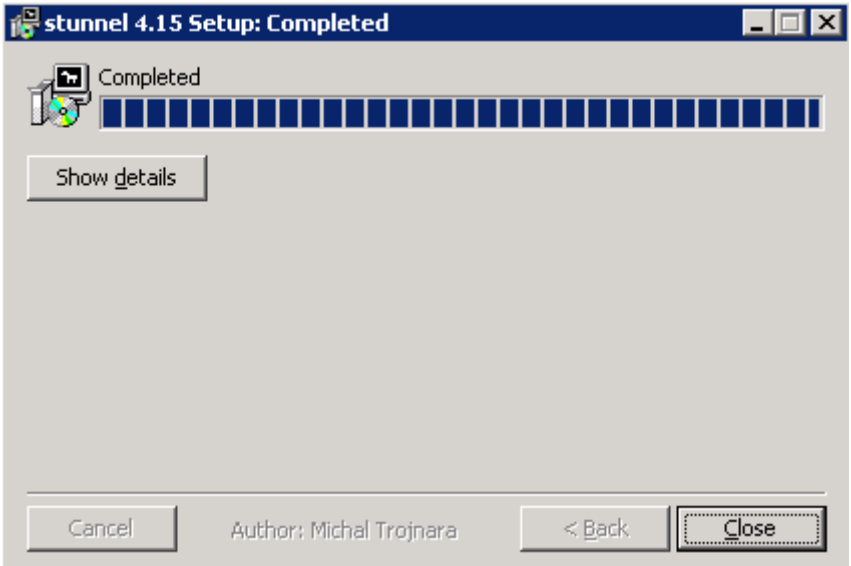

Figure 2.6. Stunnel Installation Complete

7. click **Close**.

2.2 Configure IIS Server

Complete the following steps to configure Stunnel on the IIS server in client mode:

8. select **Start > Programs > Stunnel, Edit Stunnel.conf** displaying the left screen in Figure 2.7,

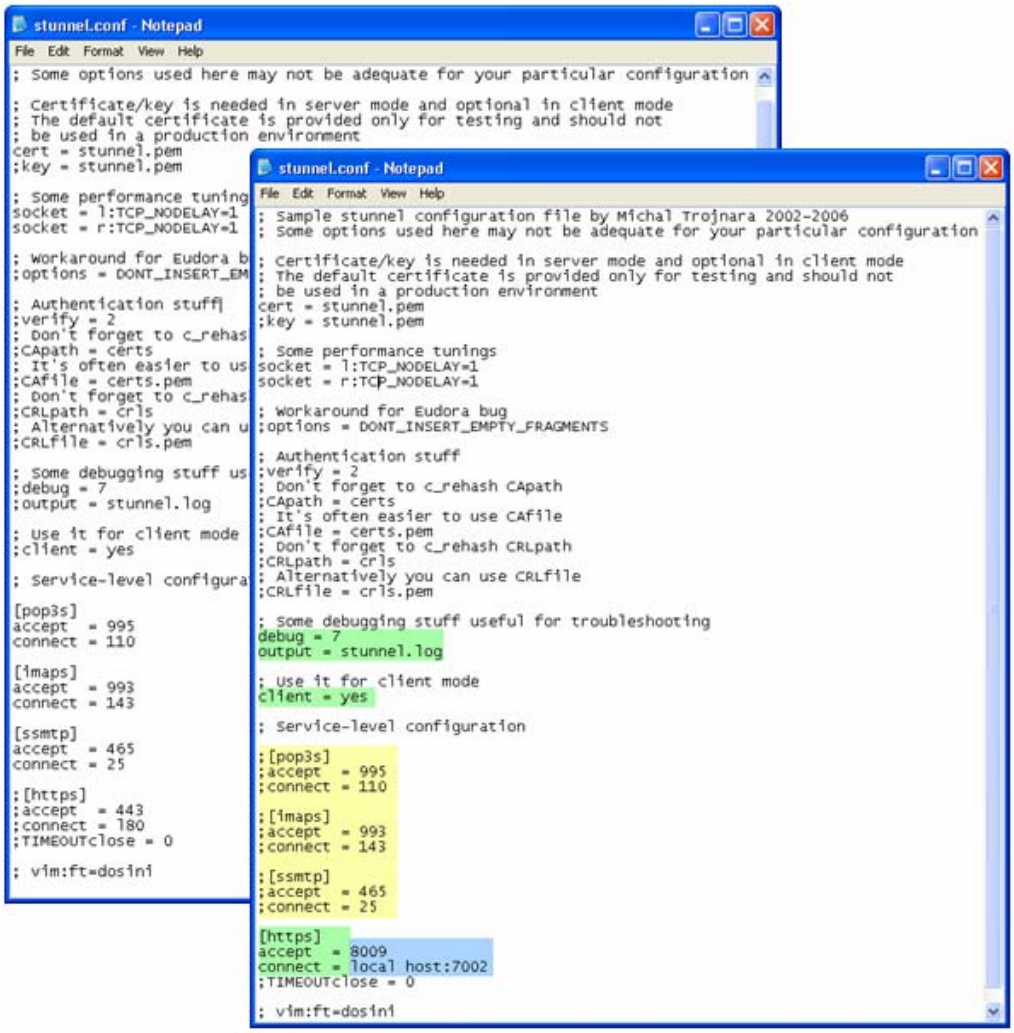

Figure 2.7. IIS Server Configuration

9. add **semicolons (;)** to the designated lines highlighted yellow, remove the **semicolons (;)** from the designated lines highlighted green, change accept and connect highlighted blue to **8009 and local host:7002** respectively, select **File**, **Save**, close window, and

Note: Ensure accept is configured to use port 8009 for ajp13 traffic. The local host should be the PHINMS Receiver Internet Protocol (IP) address.

10. select **Start > All Programs > Stunnel > Service Start**.

2.3 Configure PHINMS Receiver Service Mode

1. select **Start > All Programs > Stunnel > Edit Stunnel.conf** displaying the left screen in Figure 2.8,

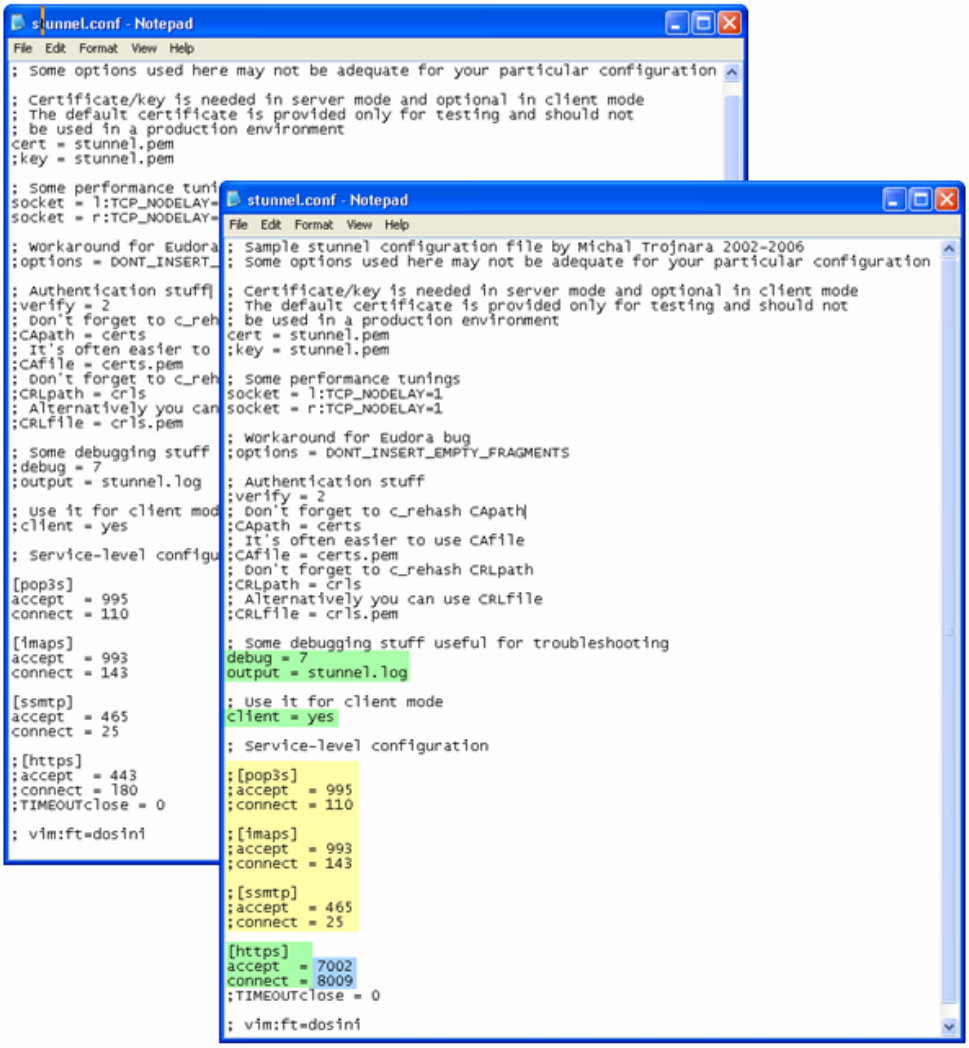

Figure 2.8. PHINMS Receiver Service Mode Configuration

2. add **semicolons (;)** to the designated lines highlighted yellow, remove the **semicolons (;)** from the designated lines highlighted green, change accept and connect highlighted blue to **7002 and connect to 8009** respectively, select **File**, **Save**, close window, and
3. select **Start > All Programs > Stunnel > Service start**.

Configure both Stunnel installations to use Self-Signed Certificates which encrypt and decrypt data between the two servers. Verify data traffic session and SSL are established. Test end-to-end from the user browser to PHINMS Sender on PHINMS Receiver.

3.0 JAKARTA

Normally the IIS can not execute servlets and Java Server Pages (JSP). Configuring IIS to use the Jakarta Internet Server Application Programming Interface (ISAPI) redirector plug-in will allow IIS to send servlet and JSP requests to Tomcat and serve them to clients. Further information on Jakarta can be located at http://tomcat.apache.org/connectors-doc/.

3.1 Pre-Jakarta Install

Complete the following steps before installing Jakarta:

1. navigate to **C:\Program Files\PhinMS\2.6\tomcat-5.0.19\conf**, select **server.xml** file,

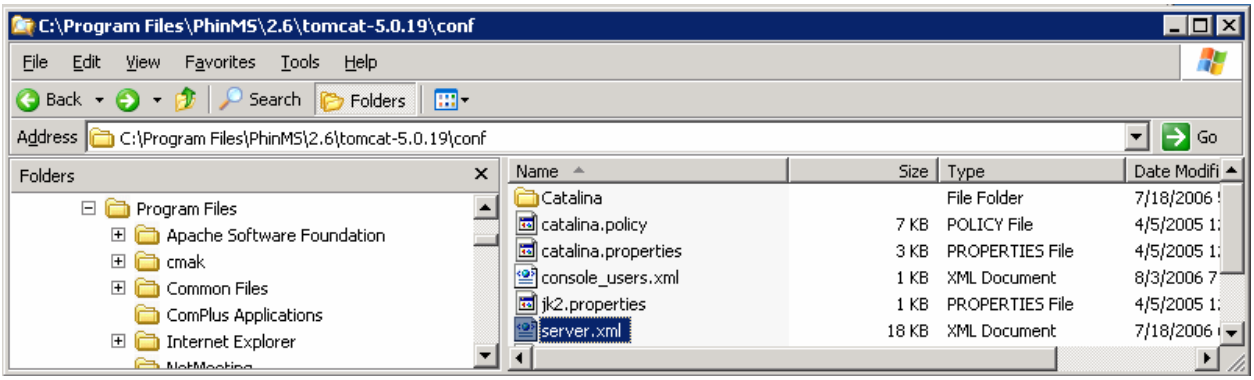

Figure 3.1. server.xml File

2. right click **server.xml** file, open with notepad displaying Figure 3.2, and

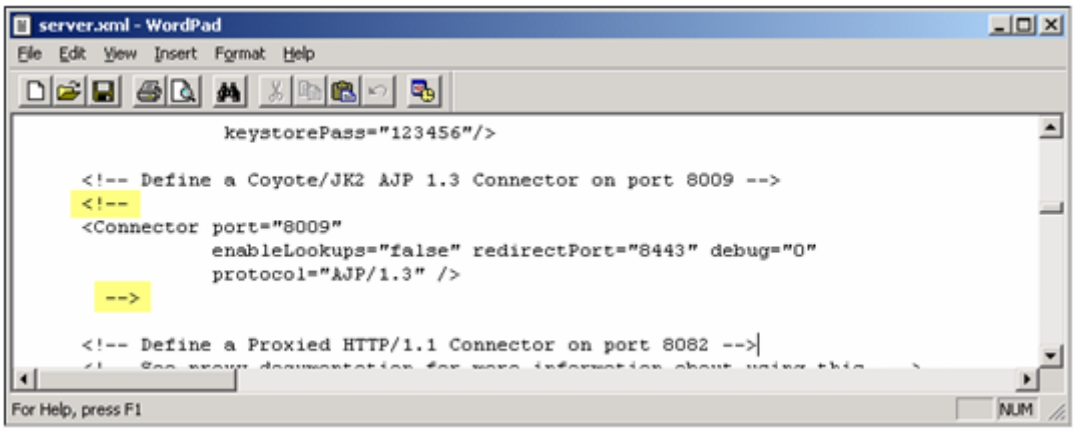

Figure 3.2. server.xml Notepad

3. search for **8009**, delete the comments highlighted in yellow shown in Figure 3.2, save the **server.xml file**, close window.

3.2 Install Jakarta

Complete the following steps to configure the Tomcat Jakarta ISAPI redirect connector on the IIS Server:

1. navigate to http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win32/jk-1.2.15/ displaying Figure 3.3,

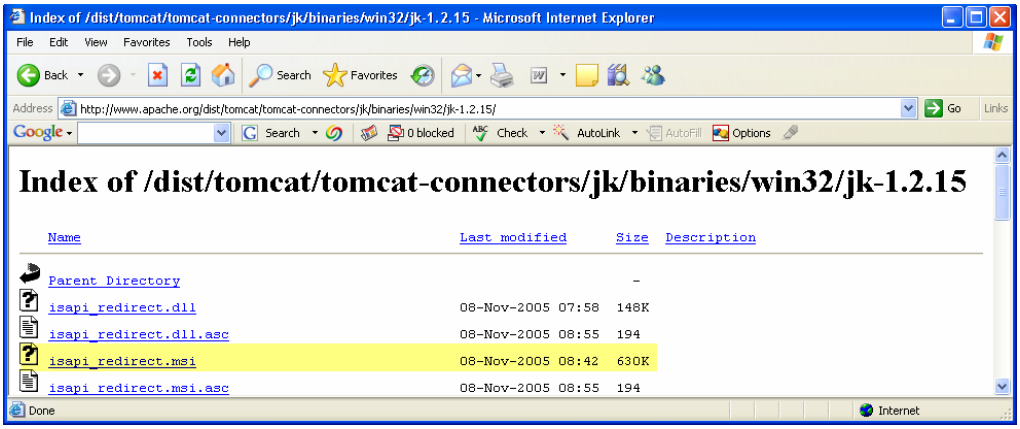

Figure 3.3. isapi_redirect.msi

2. double click the **isapi_redirect.msi** link displaying the left screen of Figure 3.4, click **Run** displaying the right screen,

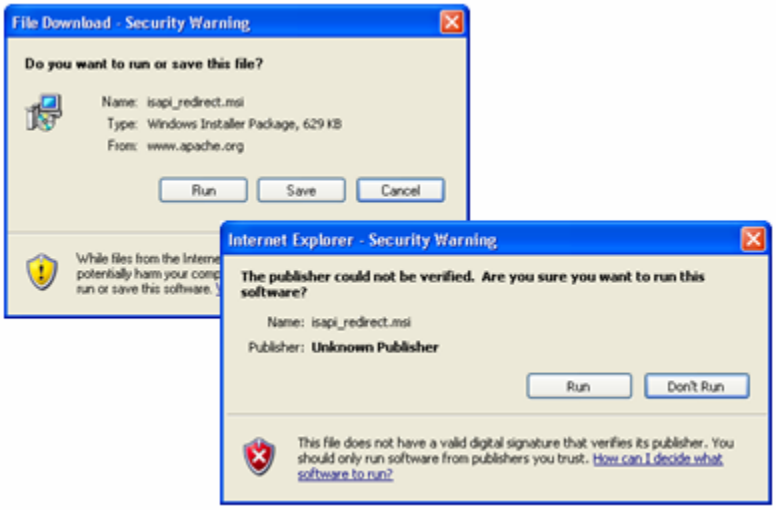

Figure 3.4. File Download

3. click **Run** displaying Figure 3.5,

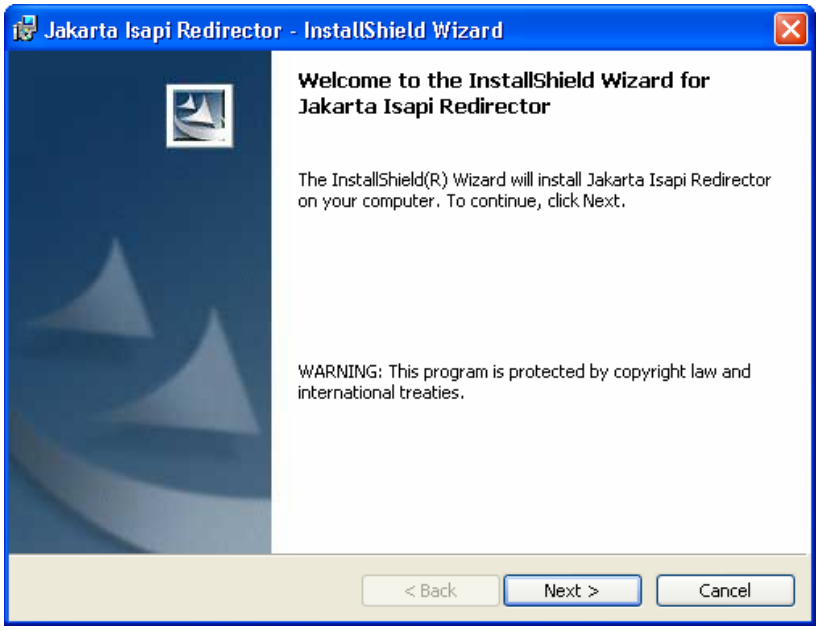

Figure 3.5. Jakarta ISAPI Redirector

4. click **Next**, displaying Figure 3.6,

Figure 3.6. License Agreement

5. read the **License Agreement**, select **I accept the terms in the license agreement**, click **Next** displaying Figure 3.7,

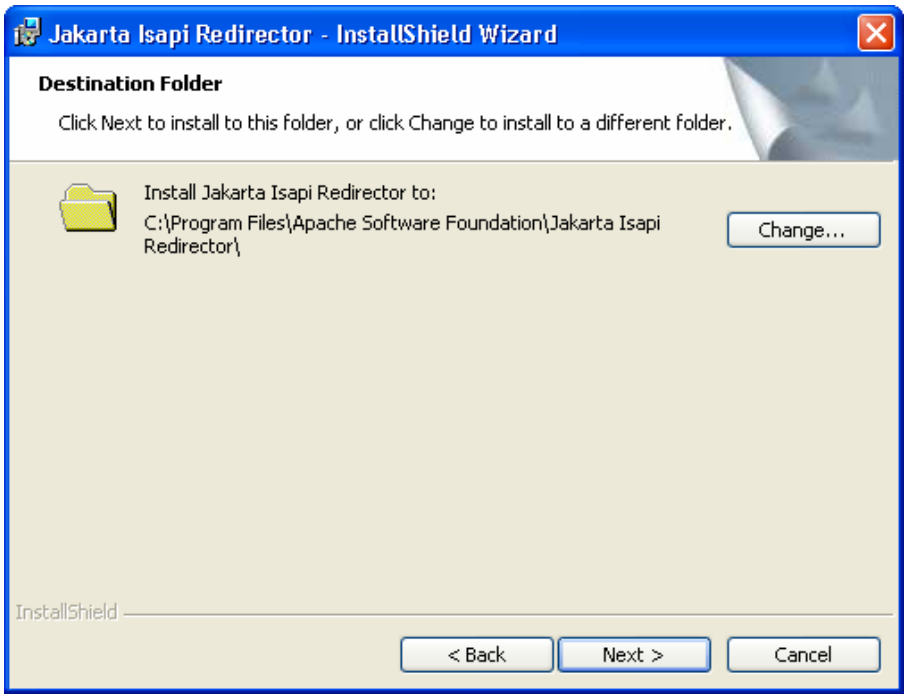

Figure 3.7. Destination Folder

6. click **Next** displaying Figure 3.8,

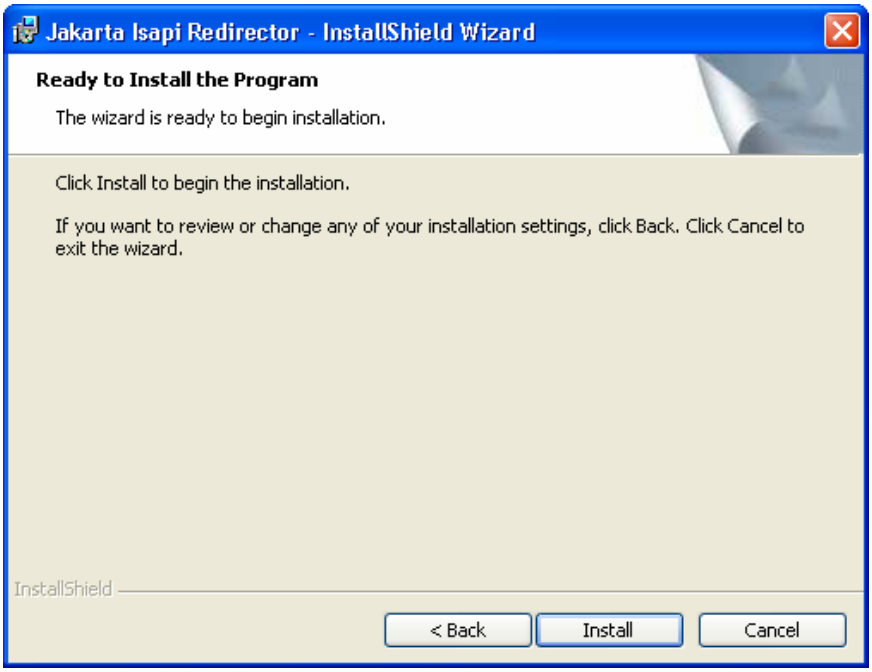

Figure 3.8. Install the Program

7. click **Install** displaying Figure 3.9, and

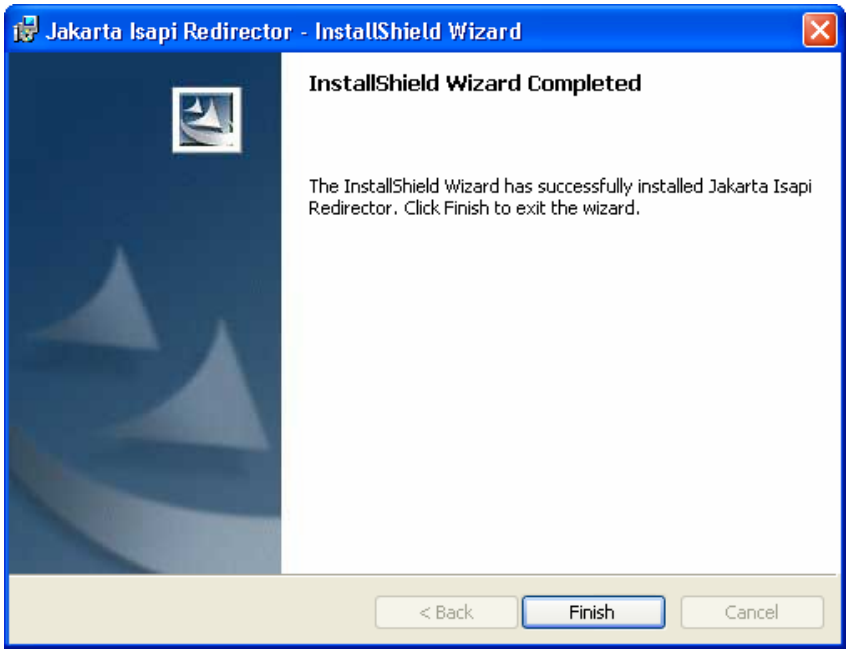

Figure 3.9. Install Complete

8. click **Finish**.

3.3 Configure Jakarta

Complete the following steps to configure Jakarta:

1. navigate to C:\Program Files\Apache Software Foundation\Jakarta Isapi Redirector\conf displaying Figure 3.10,

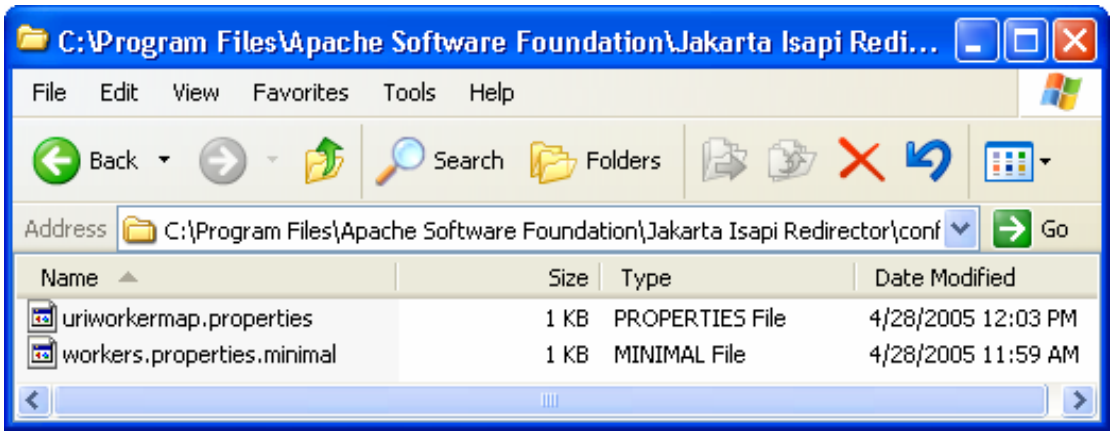

Figure 3.10. Jakarta Program Files

2. right click on **uriworkermap.properties**, select **Open** displaying Figure 3.11,

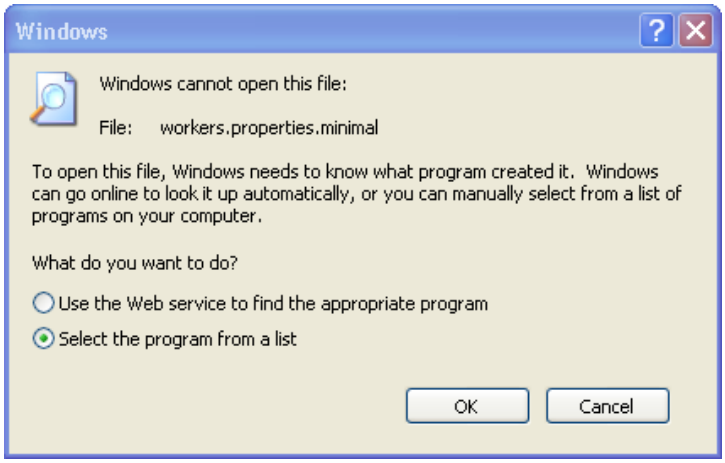

Figure 3.11. Open File

3. select **Select the program from a list**, click **OK** displaying Figure 3.12,

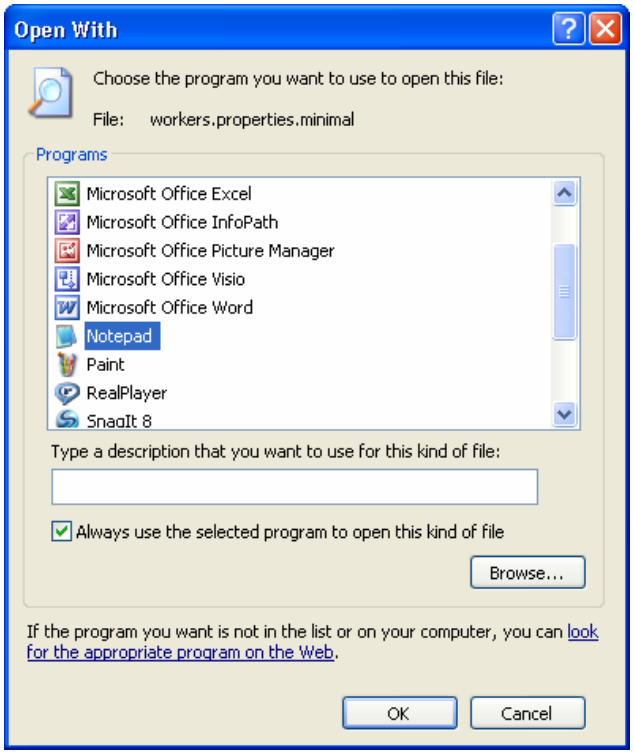

Figure 3.12. Open With

4. select **Notepad**, click **OK** displaying Figure 3.13,

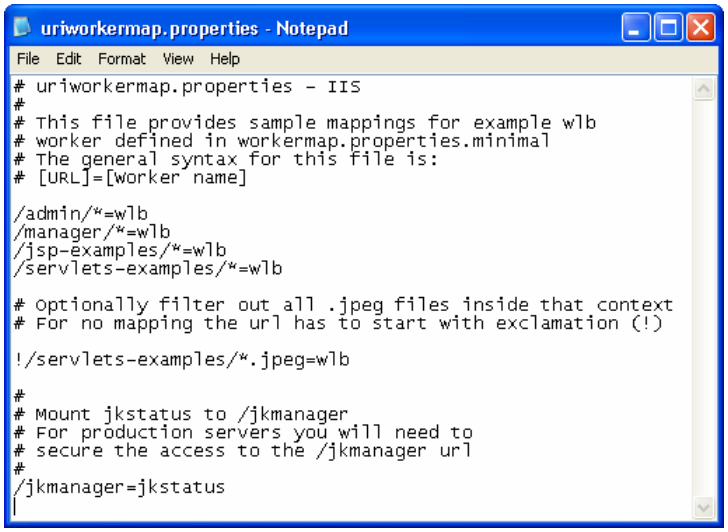

Figure 3.13. uriworkermap.properties Notepad

5. delete **/admin/*=wlb, /manager/*=wlb, /jsp-examples/*=wlb, /servlets-examples/*=wlb**, replace with **/receiver/*=wlb**, select **File**, **Save**, close Notepad,
6. navigate to **C:\Program Files\Apache Software Foundation\Jakarta Isapi Redirector\conf** displaying Figure 3.14,

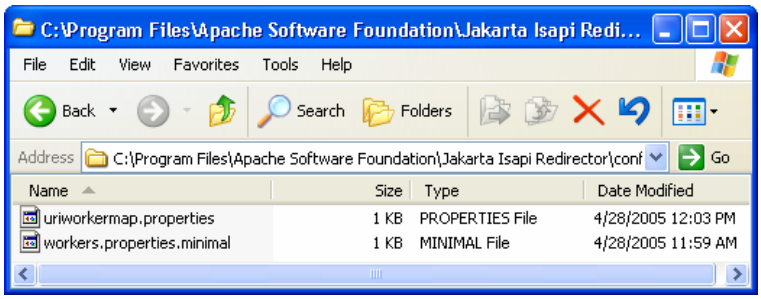

Figure 3.14. Jakarta Program Files

7. right click on **workers.properties.minimal**, select **Open**, displaying Figure 3.15,

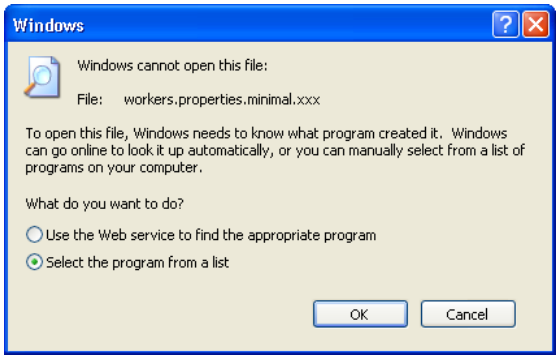

Figure 3.15. Open File

8. select **Select the program from a list**, click **OK** displaying Figure 3.17,

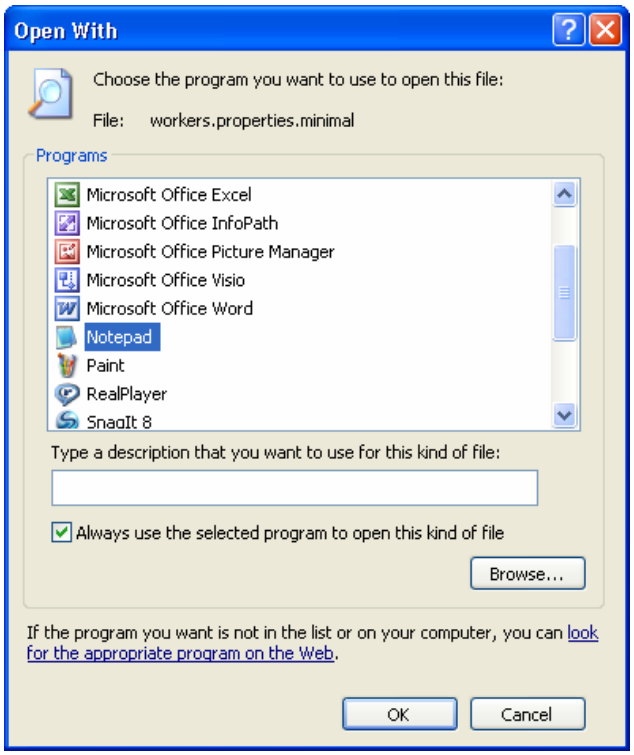

Figure 3.17. Open With

9. select **Notepad**, click **OK** displaying Figure 3.18,

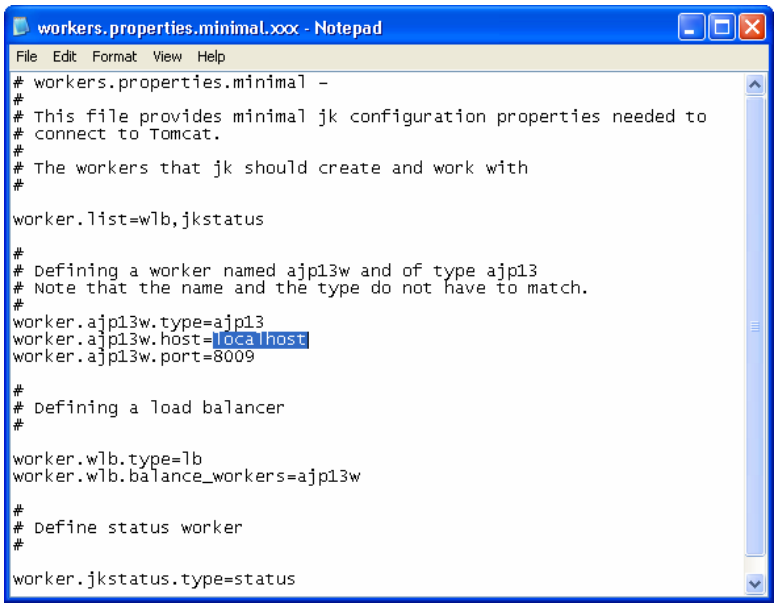

Figure 3.18. workers.properties.minimal Notepad

10. delete **localhost**, replace with the **localhost (IP) address (127.0.0.1)**, select **File**, **Save**, close Notepad,
11. select **Start > Settings > Control Panel > Administrator Tools** displaying Figure 3.19,

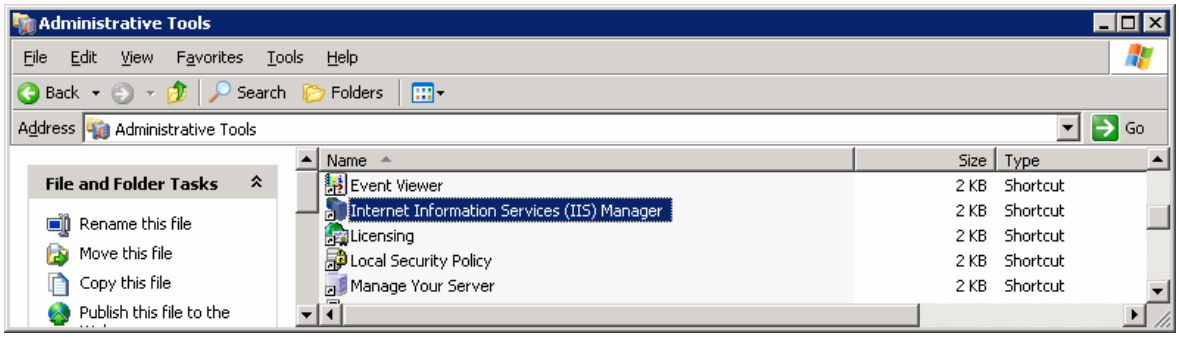

Figure 3.19. Administrative Tools

12. double click **Internet Information Services Manager (IIS)**, navigate to **Web Service Extensions** displaying Figure 3.20,

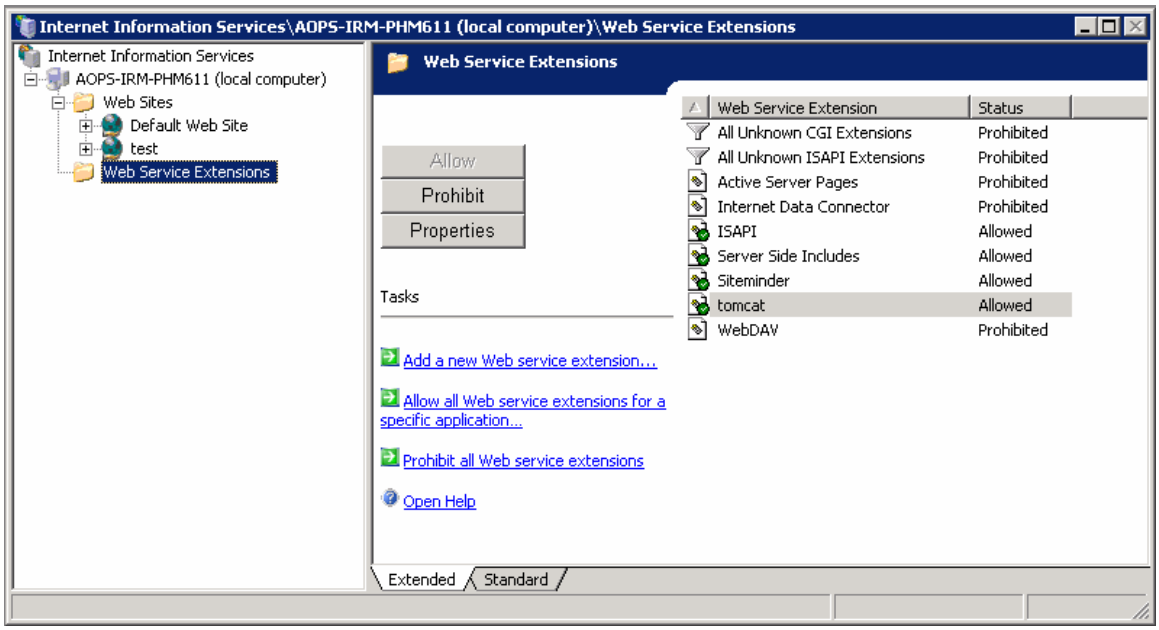

Figure 3.20. IIS Manager

13. right click on **Web Service Extensions**, select **Add a new Web service extension** displaying Figure 3.21,

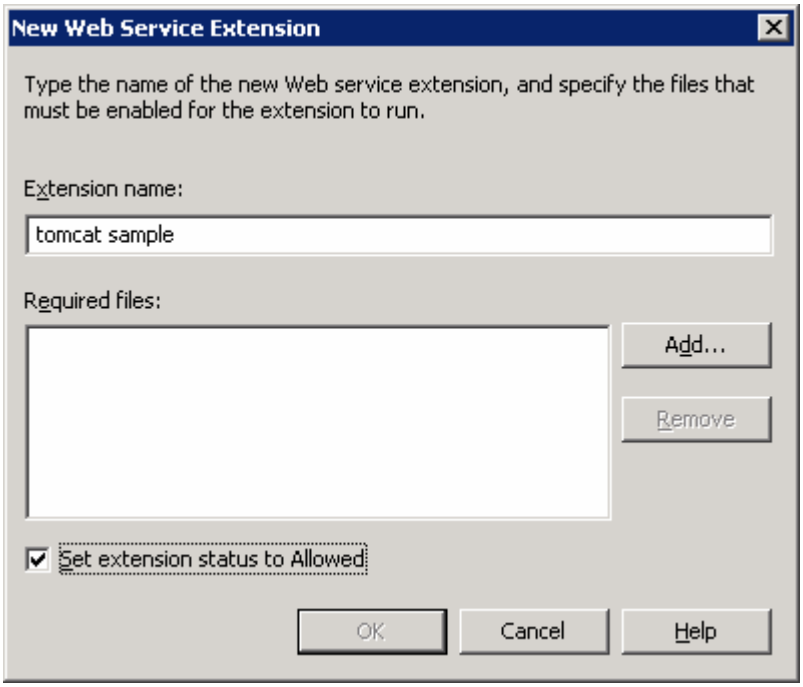

Figure 3.21. New Web Service Extension

14. enter an **Extension name**, check **Set extension status to allowed**, select **Add** displaying Figure 3.22,

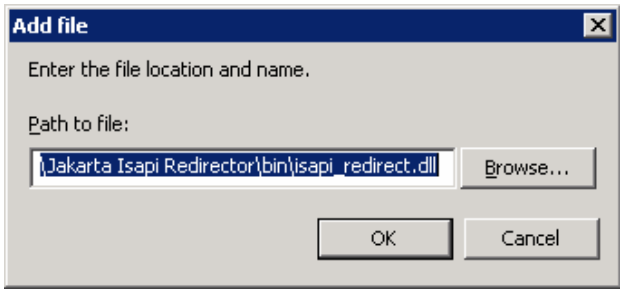

Figure 3.22. Add File

15. select **Browse**, navigate to **C:\Program Files\Apache Software Foundation\Jakarta Isapi Redirector\bin\isapi_redirect.dll,** click **OK**, **OK**, **OK** displaying Figure 3.23,

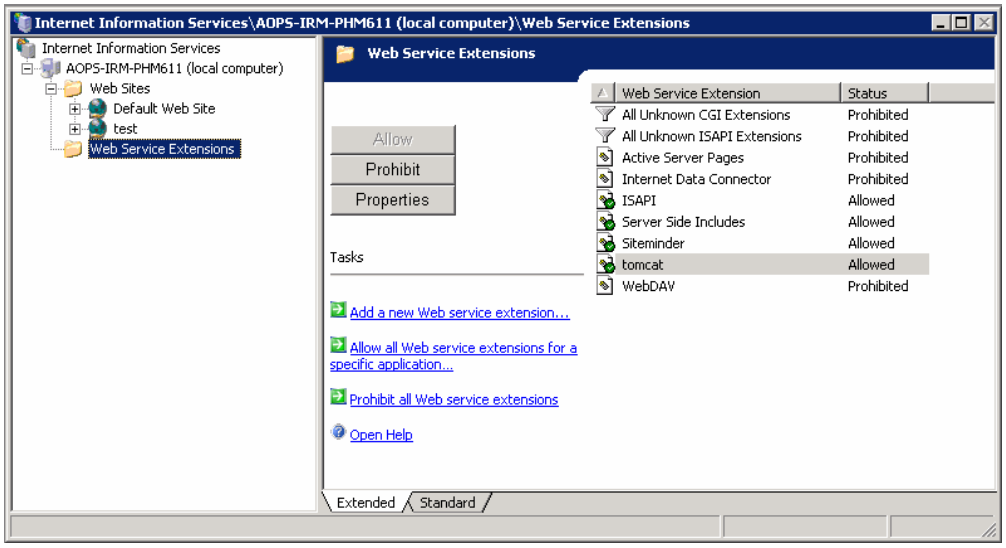

Figure 3.23. Internet Information Services

16. verify **ISAPI Web Extension** has been added, expand **Web Sites**, click on **Default Web Site**, displaying Figure 3.24,

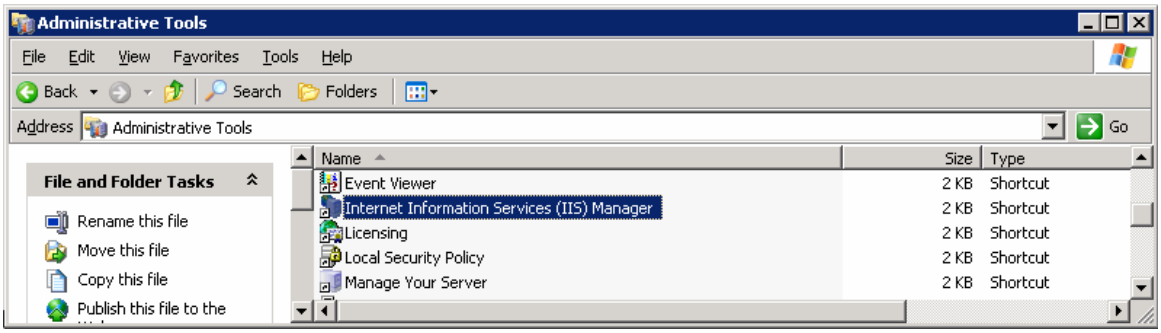

Figure 3.24. Default Web Site

17. right click on **Default Web Site**, select **Properties** displaying Figure 3.25,

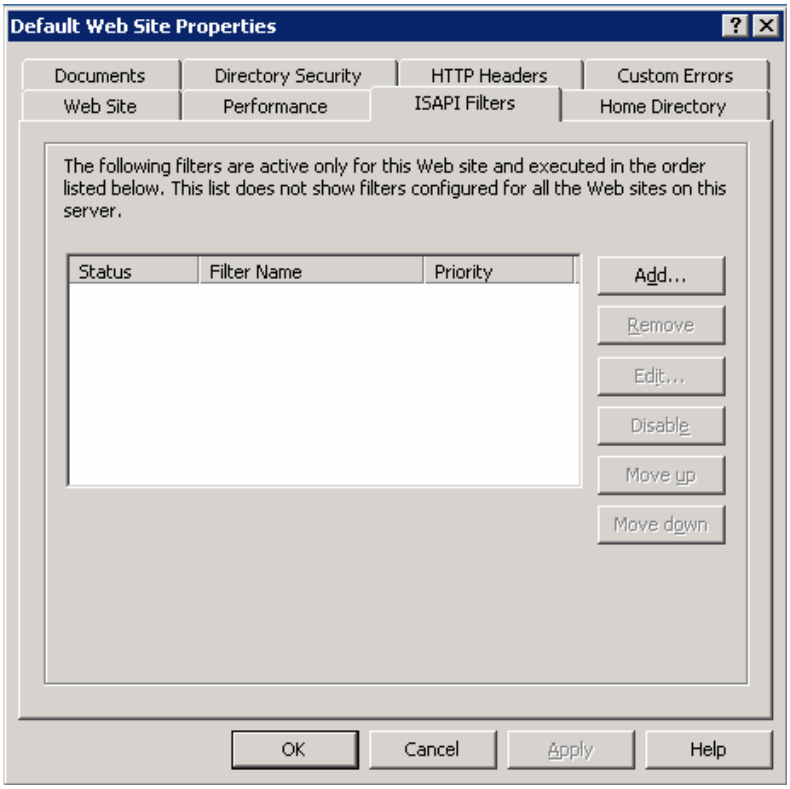

Figure 3.25. Default Web Site Properties

18. select **ISAPI Filters** tab, select **Add** displaying Figure 3.26,

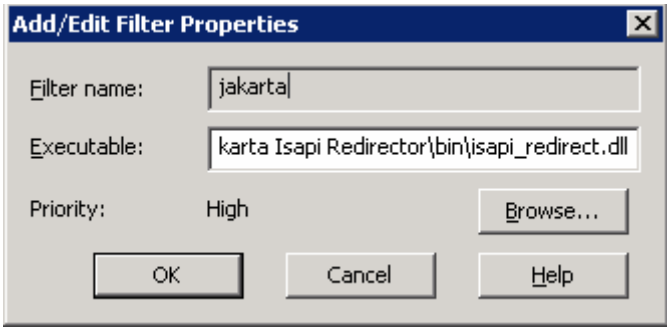

Figure 3.26. Add/Edit Filter Properties

19. enter **Filter Name**, browse to **C:\Program Files\Apache Software Foundation\Jakarta Isapi Redirector\bin\isapi_redirect.dll**, click **OK**, select **Directory Security** tab displaying Figure 3.27,

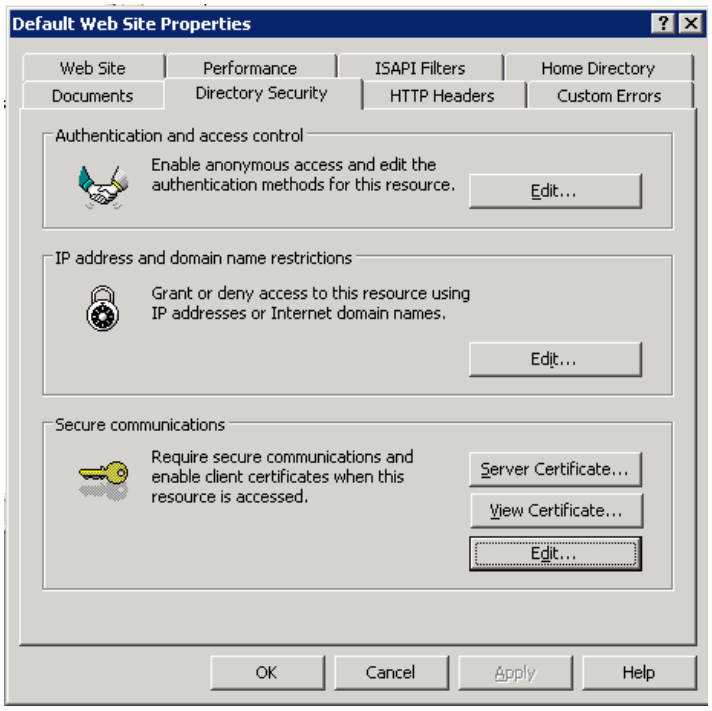

Figure 3.27. Directory Security

20. select **Edit** in the Secure communications section displaying Figure 3.28,

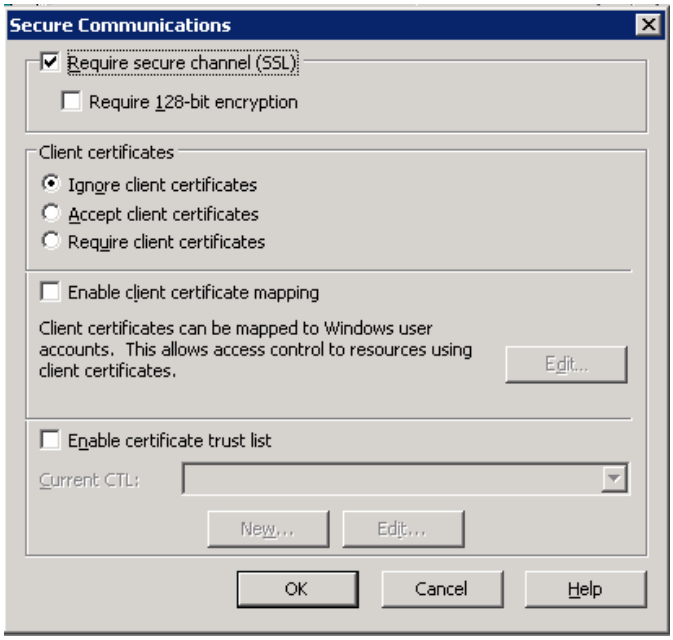

Figure 3.28. Secure Communications

21. check **Require secure channel (SSL)**, click **OK**, **OK** displaying Figure 3.29, and

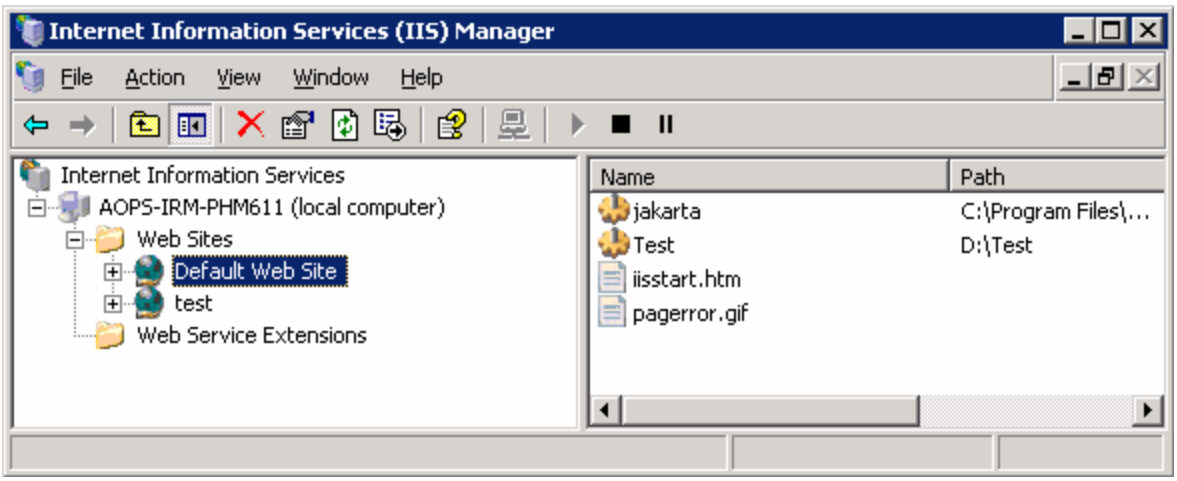

Figure 3.29. Administrative Tools

22. click ■ on the menu bar to stop and ▶ to restart the IIS services.

3.4 Test Jakarta IIS Filter

Complete the following steps to test the Jakarta IIS filter:

1. open **Internet Browser**, type the **local host of the IIS Web Server**, select **Enter** displaying Figure 3.30,

Note: Ensure https is used for the secure site and not http otherwise an error will occur.

Figure 3.30. Security Alert

2. select **Yes** displaying Figure 3.31, and

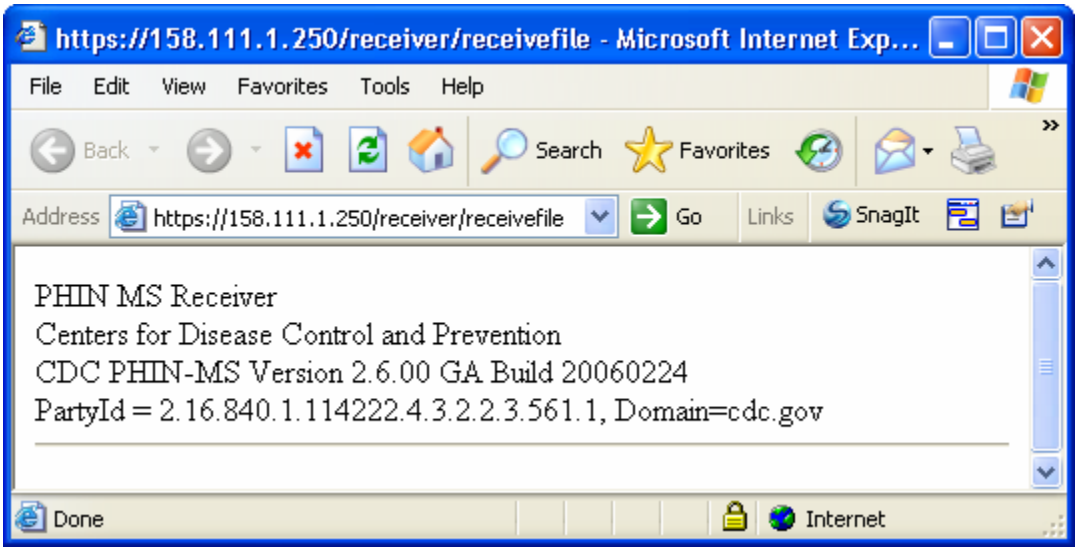

Figure 3.31. PHINMS Receiver Notification

3. close window.

4.0 CONFIGURE ONE TO ONE MAPPING

One-to-one mapping maps individual client certificates to local user accounts. The server compares the copy of the client certificate it stores with the client certificate sent by the browser. The two must be absolutely identical for the mapping to proceed. When a client gets another certificate containing all of the same user information, it must be mapped again.

4.1 Create Account

The system administrator must first create a local user account on the IIS server before completing the following steps used to configure one to one mapping:

1. locate the **Jakarta Isapi Redirector** folder using windows explorer, displaying Figure 4.1,

Figure 4.1. Jakarta Bin Folder

2. right click **Bin**, select **Sharing and Security** displaying Figure 4.2,

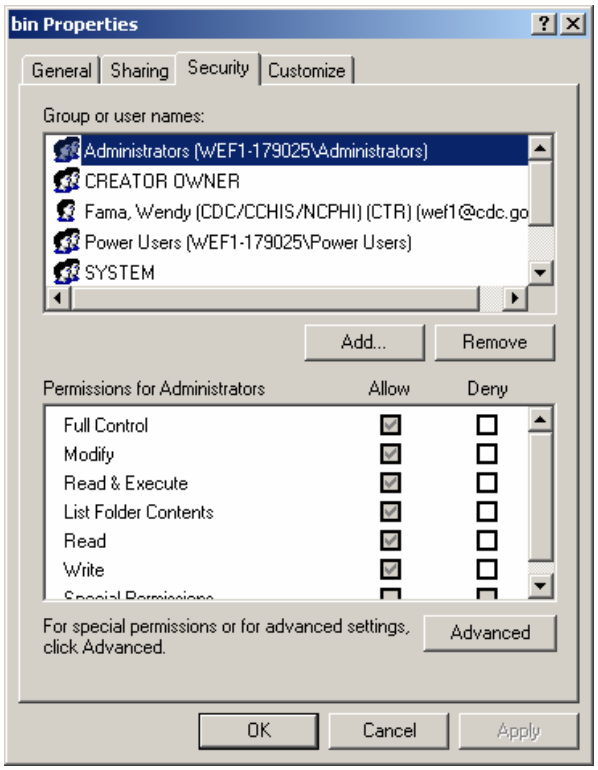

Figure 4.2. Bin Properties

3. click the **Advance** tab displaying Figure 4.3,

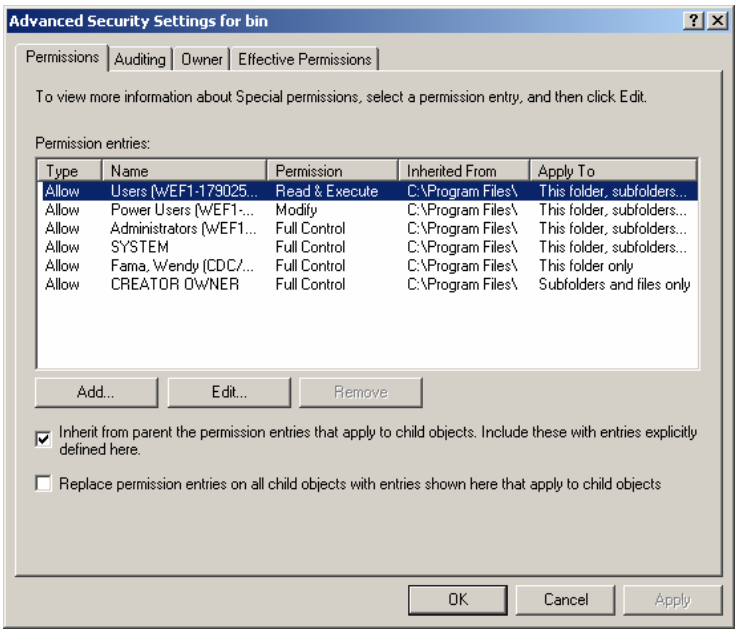

Figure 4.3. Advanced Security Setting for Bin

4. ensure all of the following **Permission Entries** are listed:

- Network Service,
- Creator Owner,
- Interactive,
- System,
- Administrator,
- User Account,
- the local account the system administrator has created for one to one mapping authentication,

5. check **Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.**, click **OK**, **OK** displaying Figure 4.4,

Figure 4.4. isapi_redirect.dll

6. right click **Isapi_redirect.dll**, select **Properties**, select the **Security** tab displaying Figure 4.5,

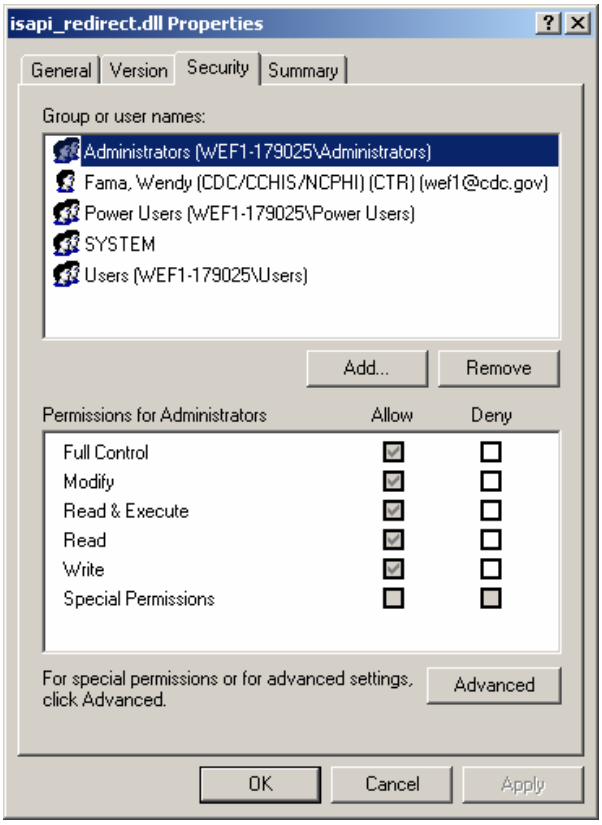

Figure 4.5. isapi_redirect.dll Properties

7. click **Add** displaying Figure 4.6,

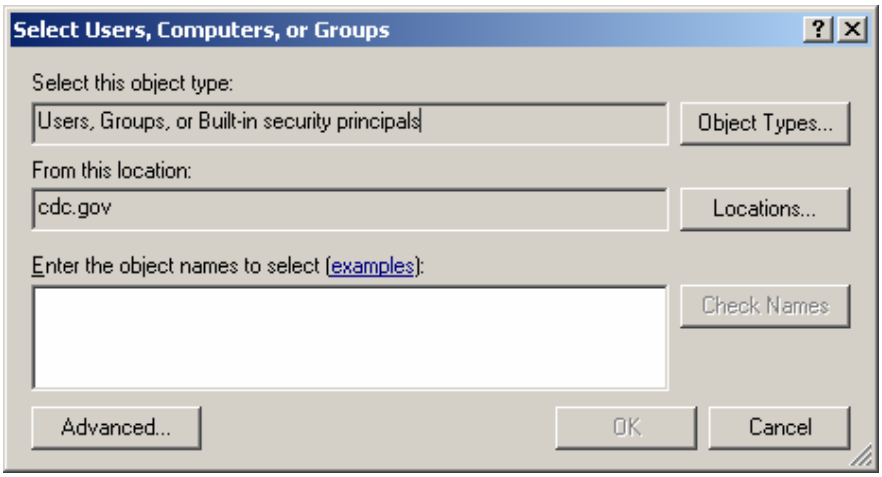

Figure 4.6. Select Users, Computers, or Groups

8. click the **Advance** tab, displaying Figure 4.7,

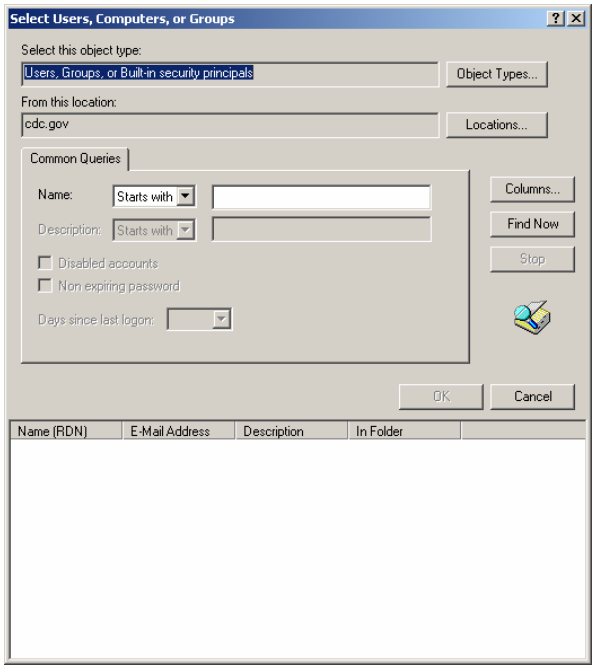

Figure 4.7. Advanced Select Users, Computers, or Groups

9. select **Find Now** populating all user account which exist on the machine, select the **User Account**, click **OK**, **OK** displaying Figure 4.8, and

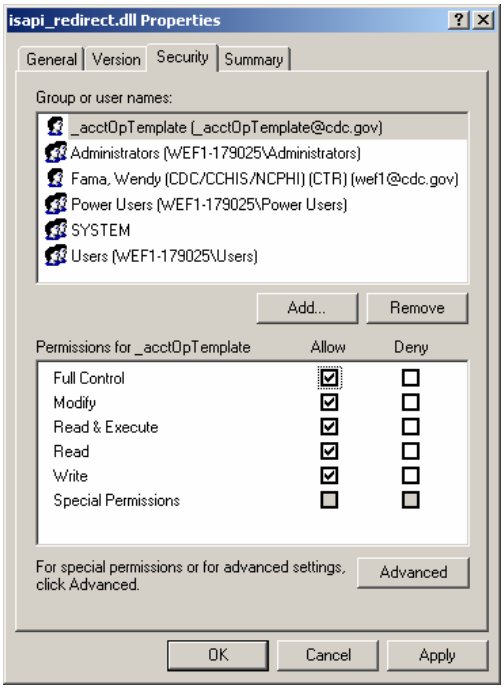

Figure 4.8. isapi_redirect.dll Properties

10. click **Full Control**, click **OK**.

4.2 Configure Jakarta Isapi

The purpose of one to one mapping is to secure individual communications between the source and the destination. One to one mapping uses the individual user account mapped to a client certificate to add additional security. One to one mapping is configured on the IIS server.

1. select **Start > Settings > Control Panel > Administrator Tools** displaying Figure 4.9,

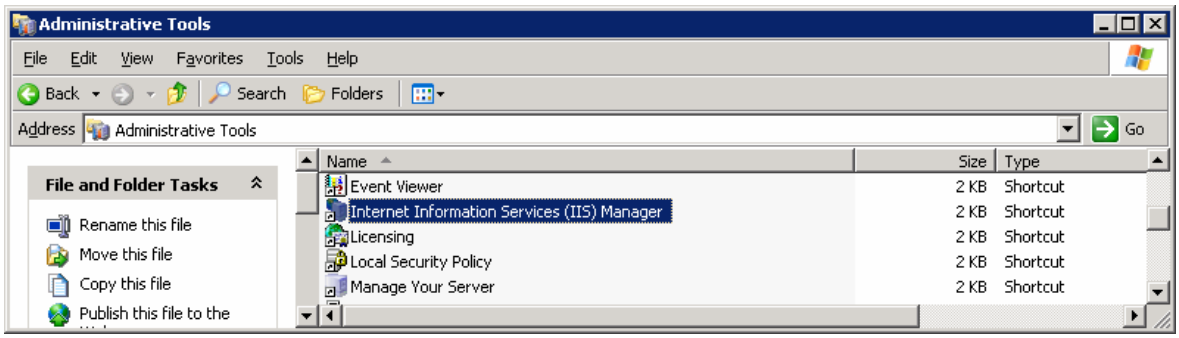

Figure 4.9. Administrative Tools

2. double click on **Internet Information Service (IIS) Manager** displaying Figure 4.10,

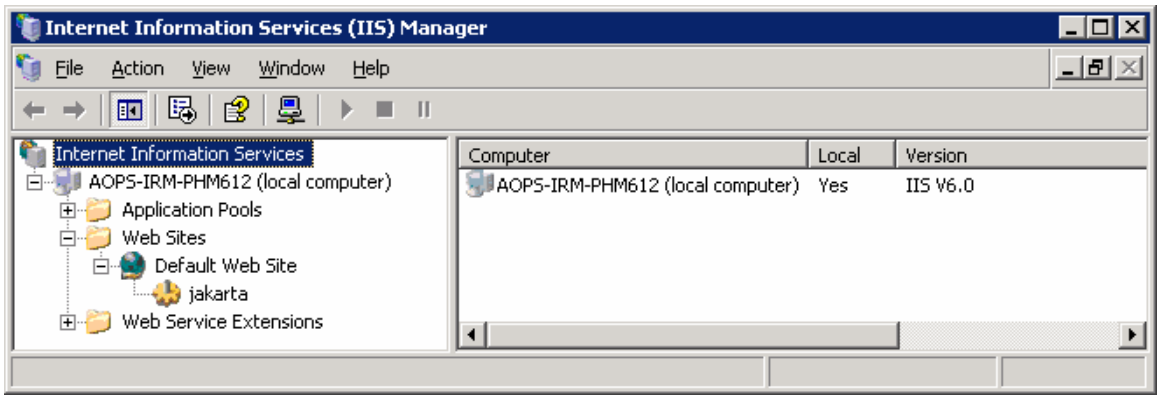

Figure 4.10. Internet Information Services (IIS) Manager

3. right click the **Default Web Site**, select **Properties** displaying Figure 4.11,

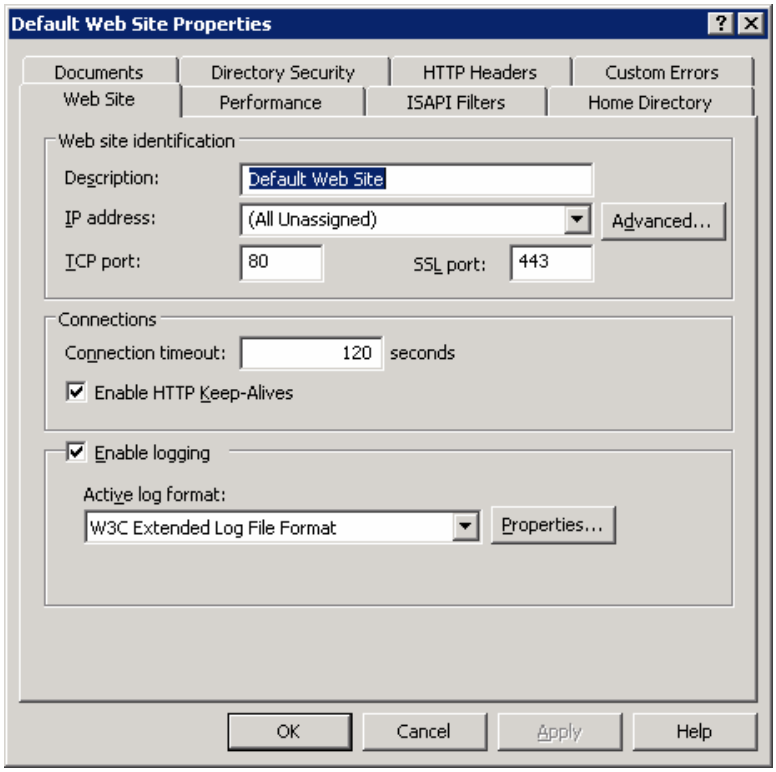

Figure 4.11. Default Web Site Properties

4. select the **Directory Security** tab displaying Figure 4.12,

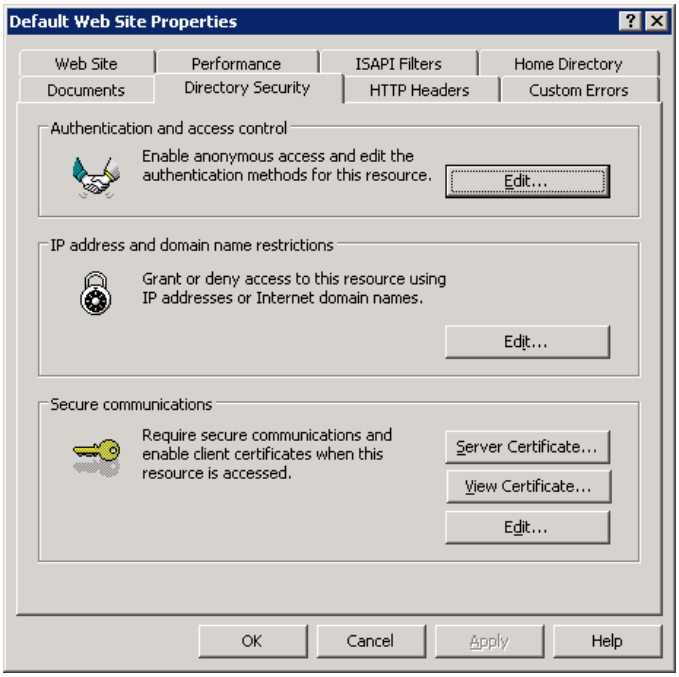

Figure 4.12. Directory Security

5. select **Edit** under the **Authentication and access control** displaying Figure 4.13,

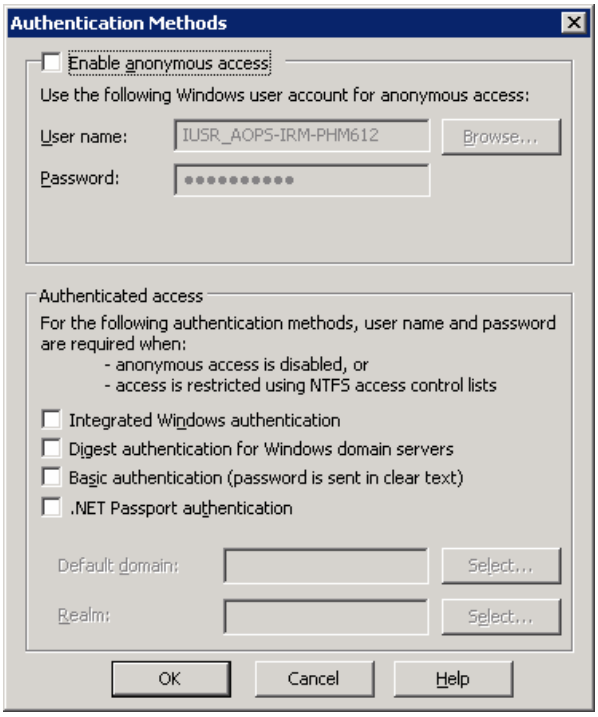

Figure 4.13. Authentication Methods

6. uncheck all **check boxes**, click **OK** returning to the Default Web Site Properties screen, click **Edit** under **Secure communications** displaying Figure 4.14,

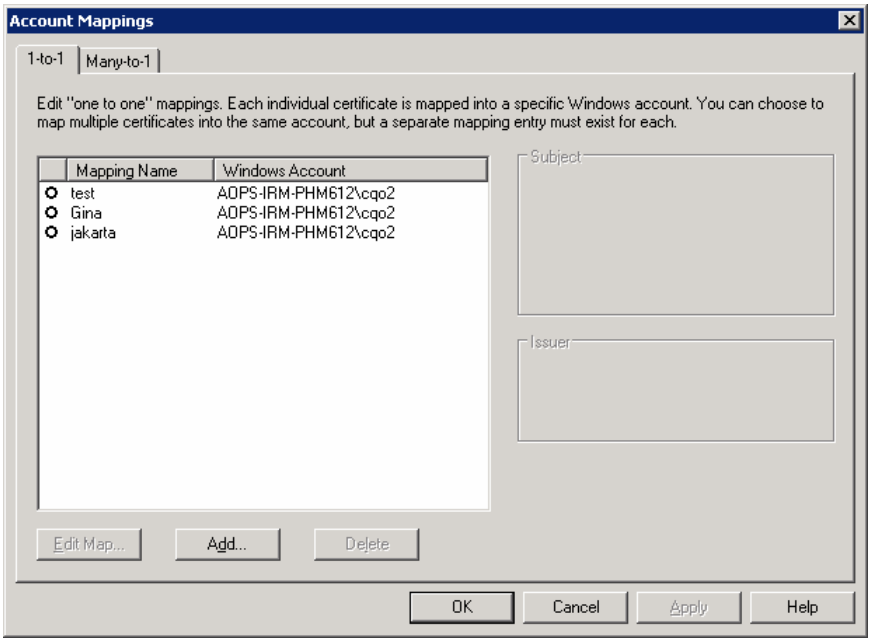

Figure 4.14. Account Mappings

7. click **Add** to map the user account with the certificate for authentication in the one to one mapping configuration displaying Figure 4.15,

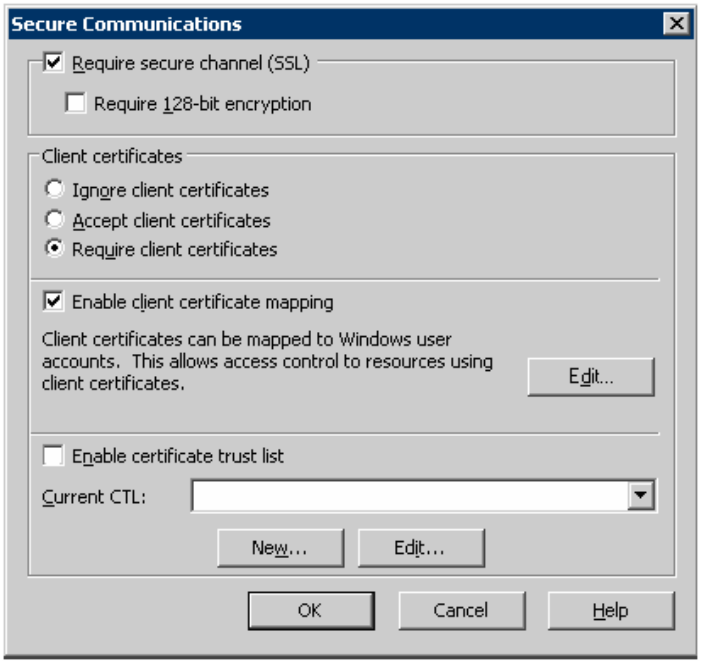

Figure 4.15. Secure Communications

8. ensure **Require secure channel (SSL)**, **Required client certificates**, **Enable client certificate mapping** is selected, click **Edit** on the far right-hand side of the screen displaying Figure 4.16,

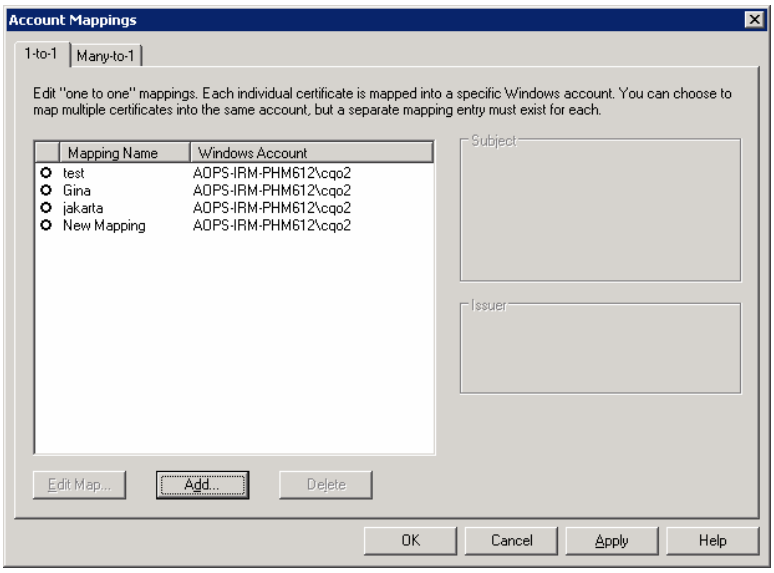

Figure 4.16. Account Mappings

9. select **Add** displaying Figure 4.17,

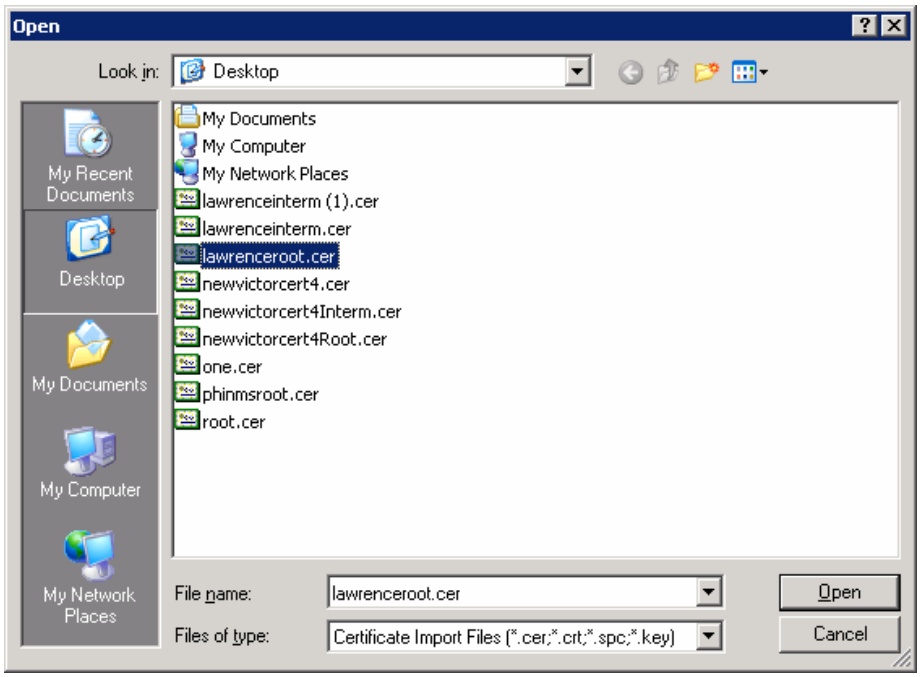

Figure 4.17. Open

10. select the **Certificate** used to secure this communication method, click **Open** displaying Figure 4.18,

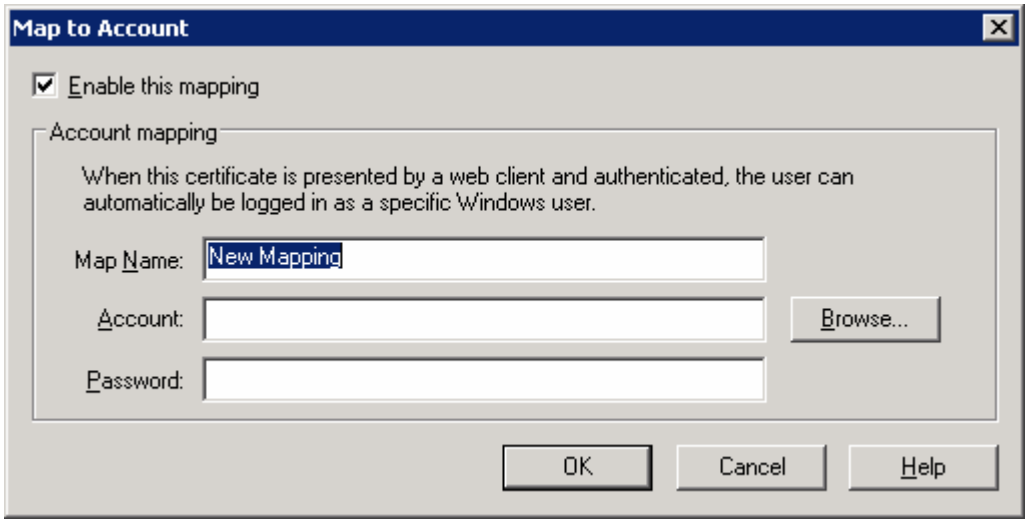

Figure 4.18. Map To Account

11. place a check in the box next to **Enable this mapping**, enter the **Map Name**, select **Browse**, search for **account** to map, enter the **Password**, click **OK**, displaying Figure 4.19,

Figure 4.19. Confirm Password

12. enter **Password** for confirmation, click **OK**, **OK** displaying Figure 4.20,

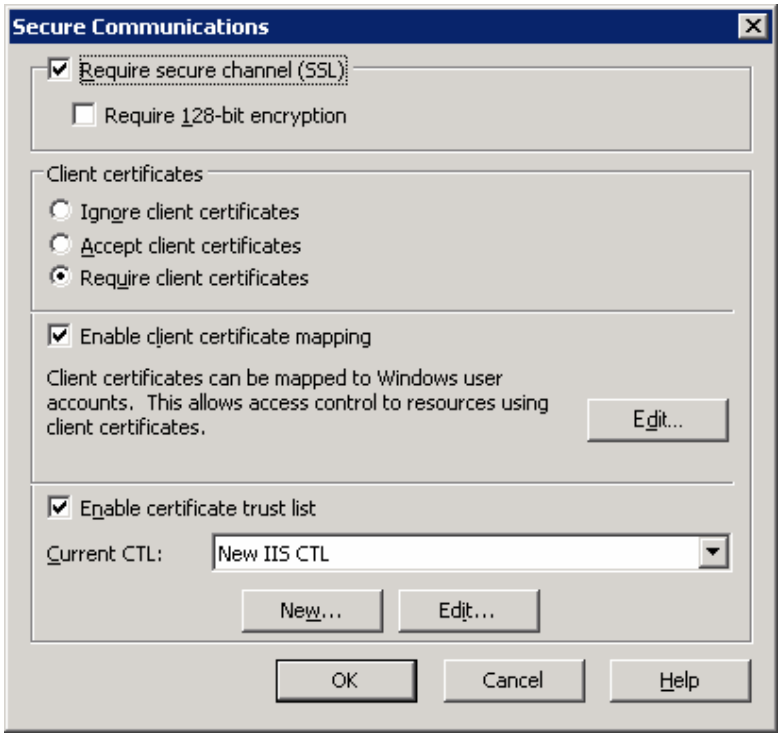

Figure 4.20. Secure Communications

13. check **Enable client certificate trust list**, select **New IIS CTL** from the drop-down list, click **OK** displaying Figure 4.21,

Figure 4.21. Certificate Trust List Wizard

14. click **Next** displaying Figure 4.22,

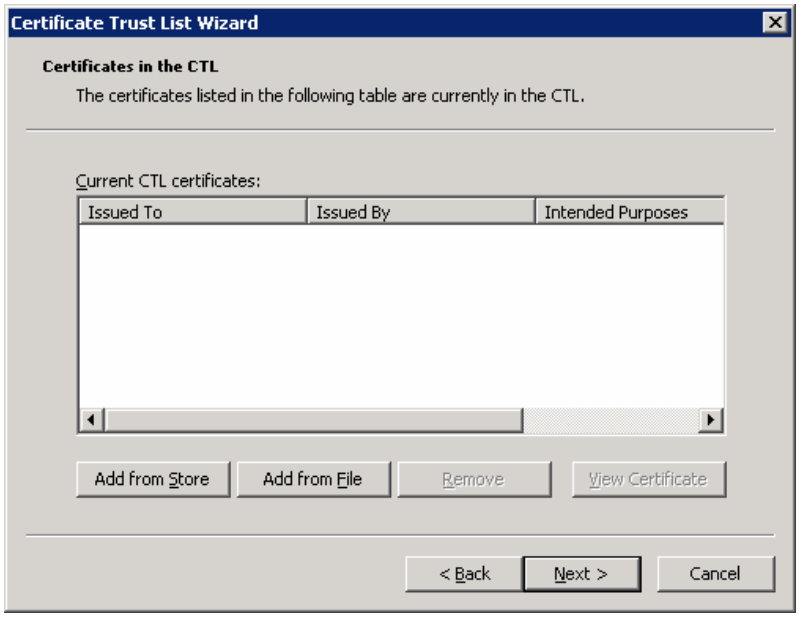

Figure 4.22. Certificates in the CTL

15. select **Add from Store** or **Add from File** displaying Figure 4.23,

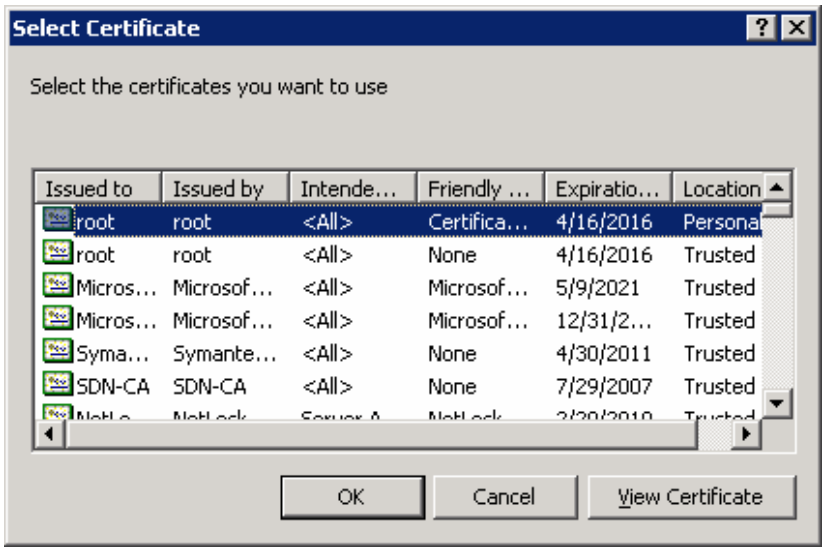

Figure 4.23. Select Certificate

16. select **Certificate**, click **OK** displaying Figure 4.24,

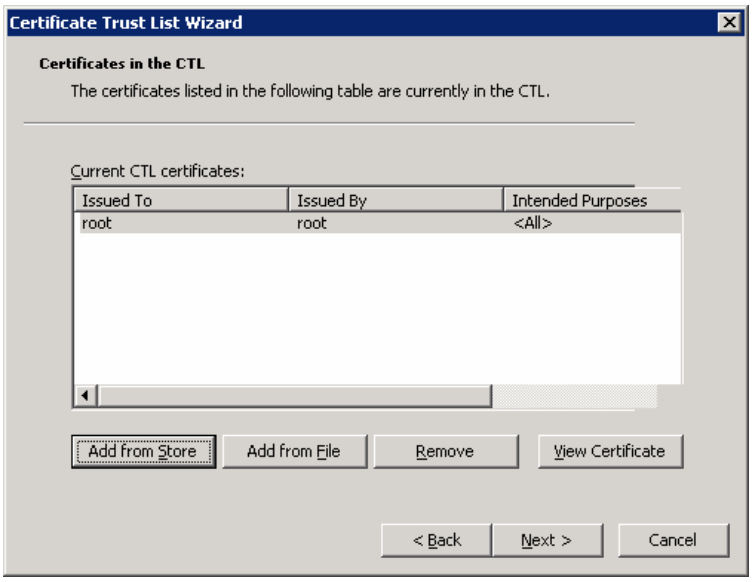

Figure 4.24. Certificate Trust List Wizard

17. select **Next** displaying Figure 4.25,

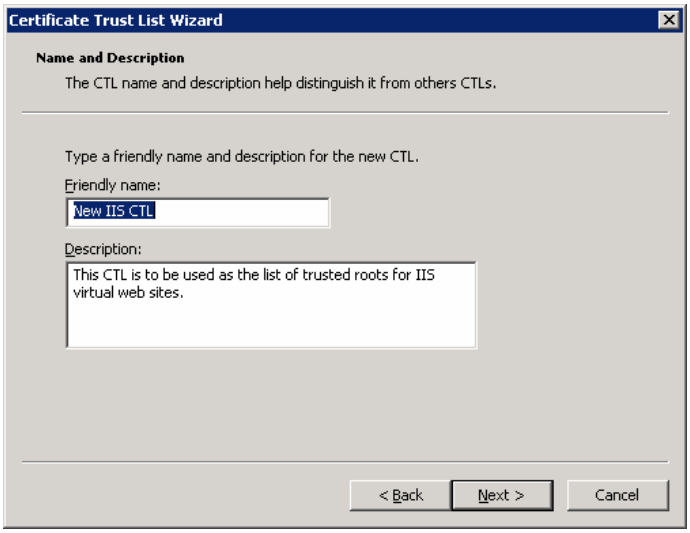

Figure 4.25. Certificate Description

18. enter **Description** for the certificate trust list, click **Next** displaying Figure 4.26,

Figure 4.26. Wizard Complete

19. click **Finish** displaying Figure 4.27,

Figure 4.27. Wizard Success

20. click **OK** displaying Figure 4.28,

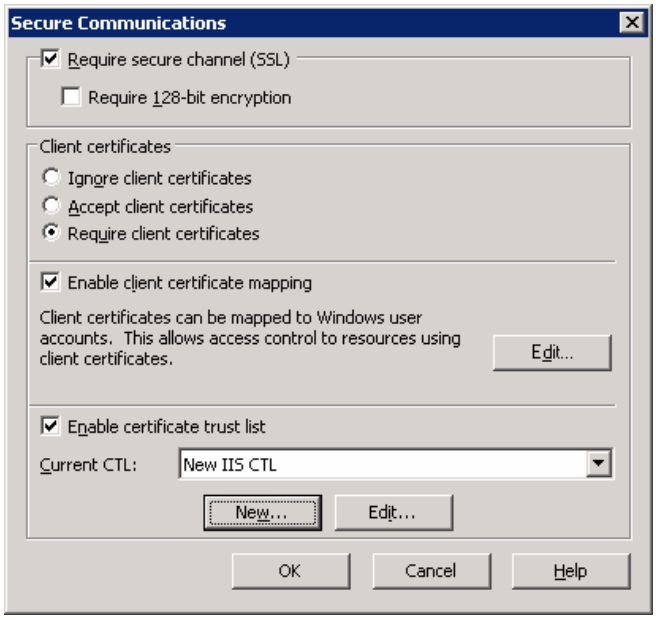

Figure 4.28. Secure Communications

21. click **OK** displaying Figure 4.29,

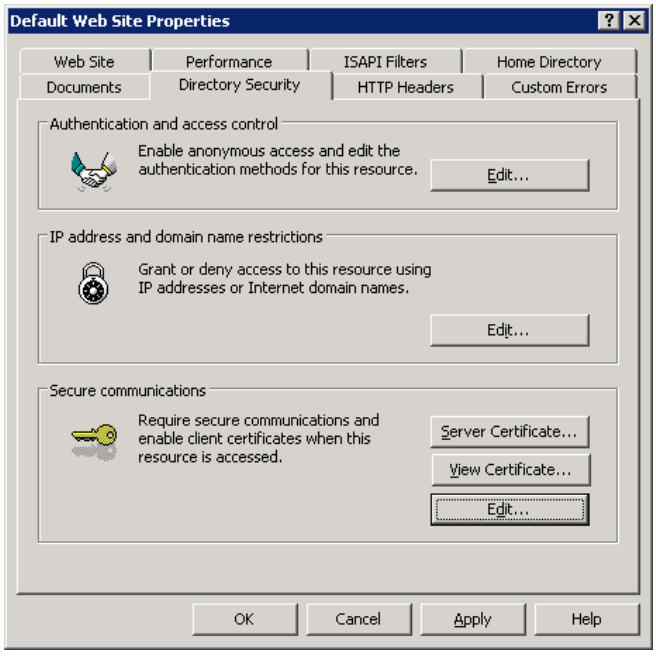

Figure 4.29. Default Web Site Properties

22. click **OK** displaying Figure 4.30,

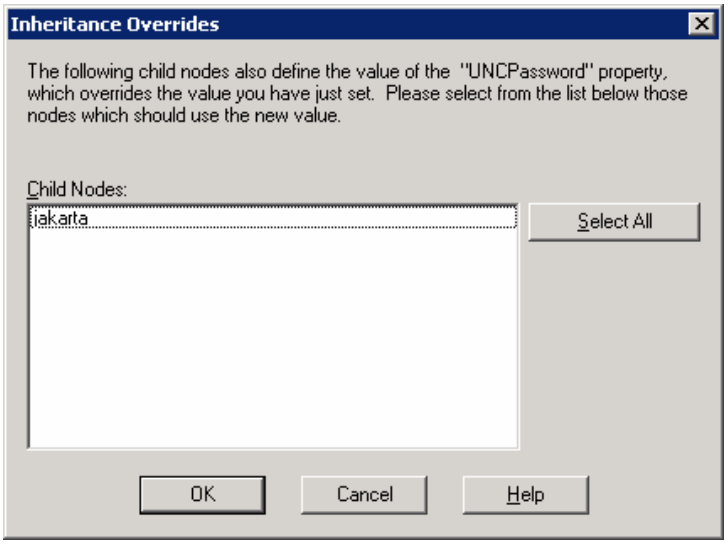

Figure 4.30. Inheritance Overrides

23. click **Select All**, click **OK** displaying Figure 4.31,

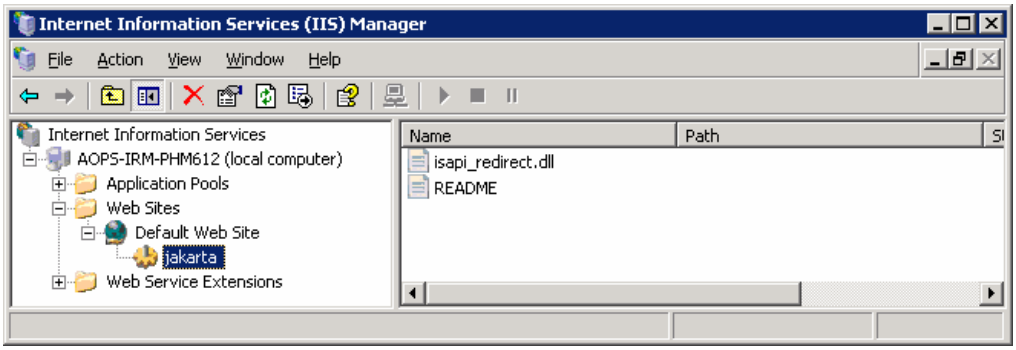

Figure 4.31. Internet Information Services (IIS) Manager

24. right click **Jakarta**, select **Properties,** select the **Directory Security** tab displaying Figure 4.32,

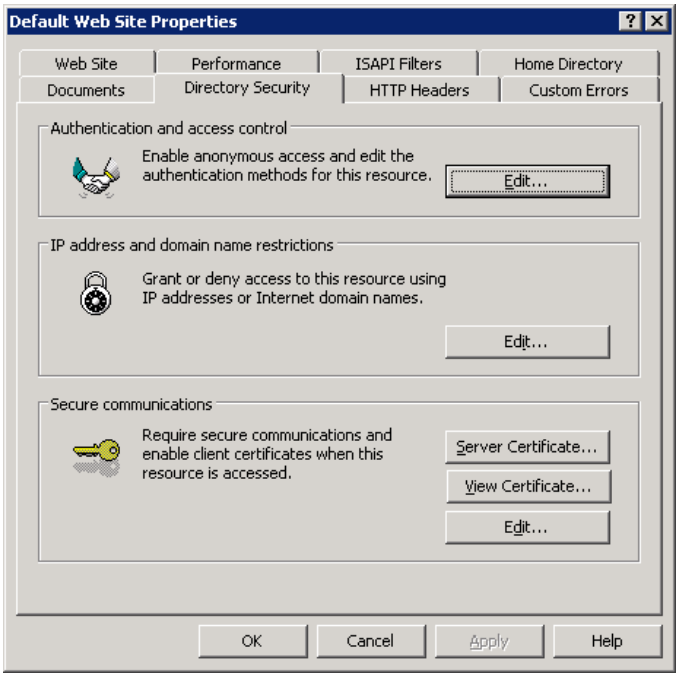

Figure 4.32. Authentication and Access Control

25. select **Edit** under **Authentication and access control** displaying Figure 4.33,

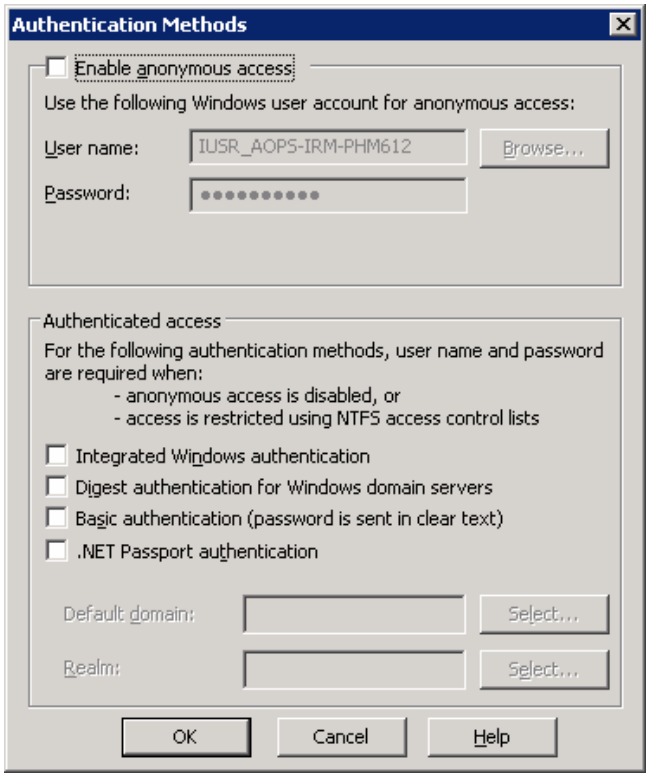

Figure 4.33. Authentication Methods

26. deselect all **Check Boxes**, click **OK** displaying Figure 4.34, and

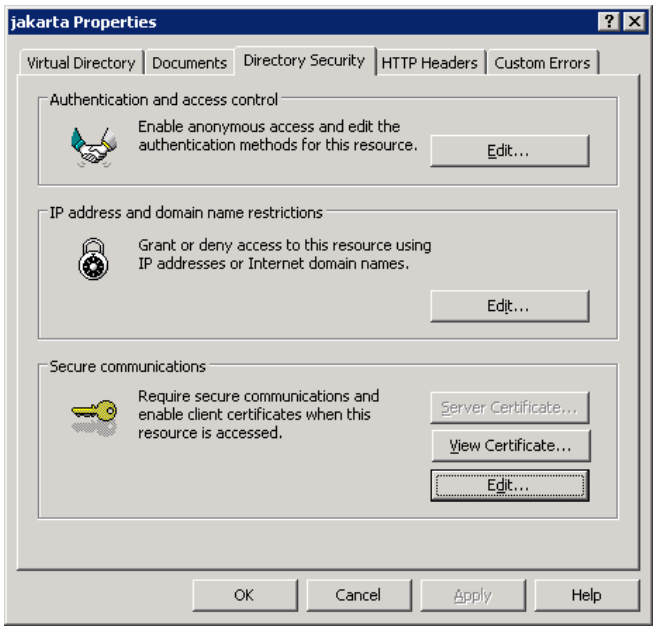

Figure 4.34. Jakarta Properties

27. click **OK**.

4.3 Test One to One Mapping

1. open **Internet Browser**, type URL https://localhost/receiver/receivefile ,select **Go** displaying Figure 4.35,

Figure 4.35. Security Alert

2. select **Yes** displaying Figure 4.36,

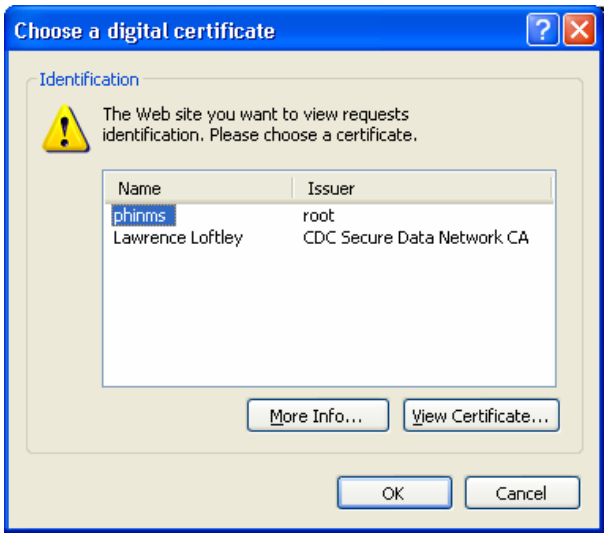

Figure 4.36. Choose a Digital Certificate

3. select the **Digital Certificate**, click **OK** displaying Figure 4.37,

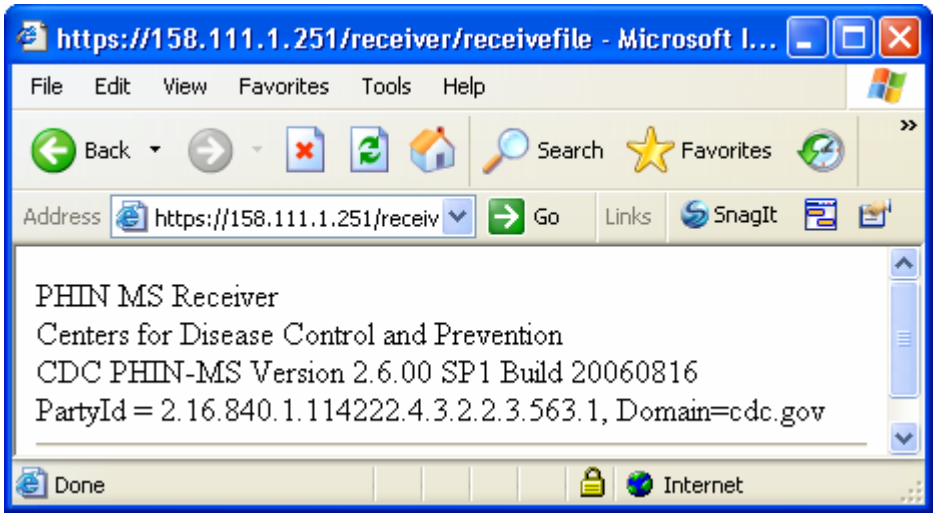

Figure 4.37. Test Successful Notification

Note: An error will occur when an invalid Digital Certificate is used on the receiver displaying Figure 4.38.

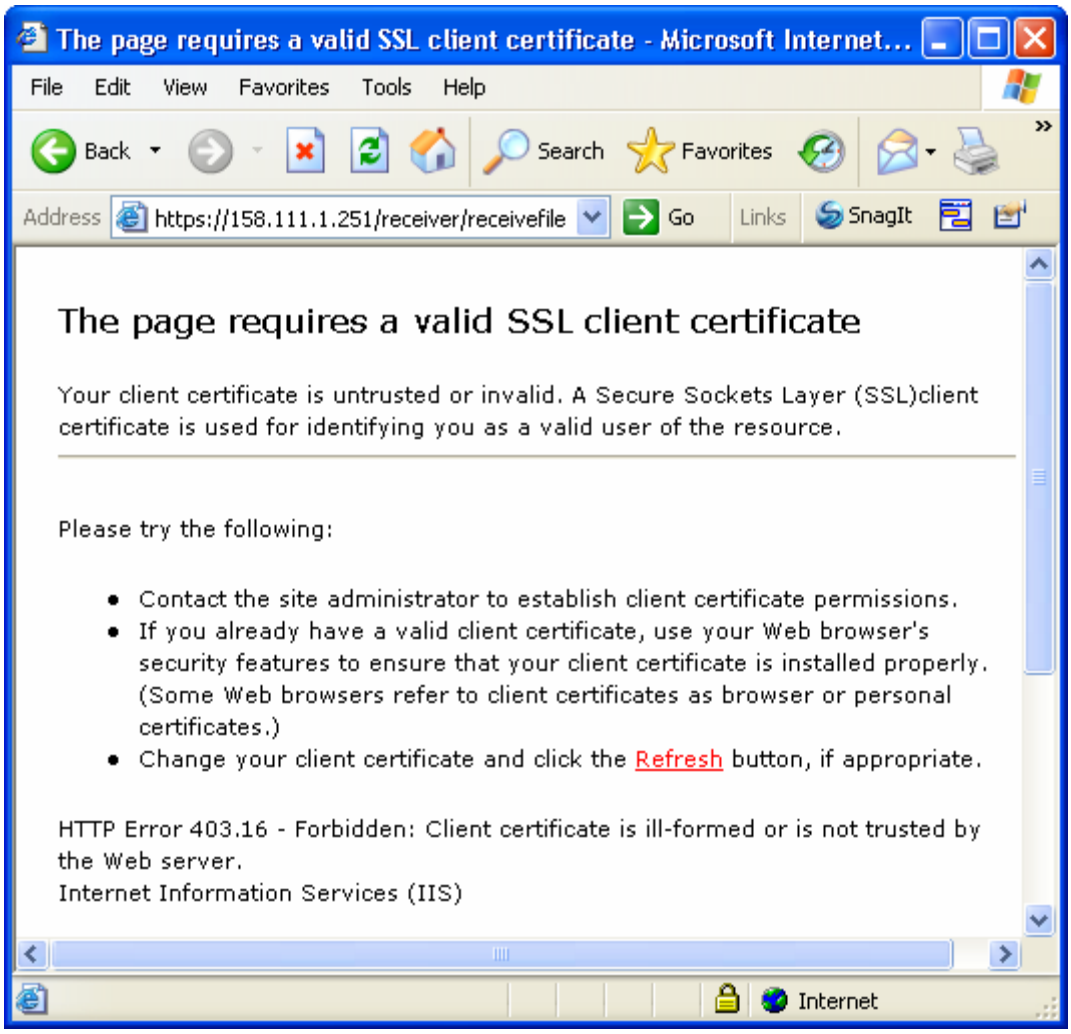

Figure 4.38. Valid SSL Client Certificate Required

5.0 SECURE SOCKET LAYERS

5.1 Download Openssl

The Openssl application should be installed on a single workstation. Complete the following steps to download Openssl:

1. create a folder on the root directory **C:\Openssl**,
2. navigate to http://www.stunnel.org/download/stunnel/win32/openssl-0.9.7/, displaying Figure 5.1,

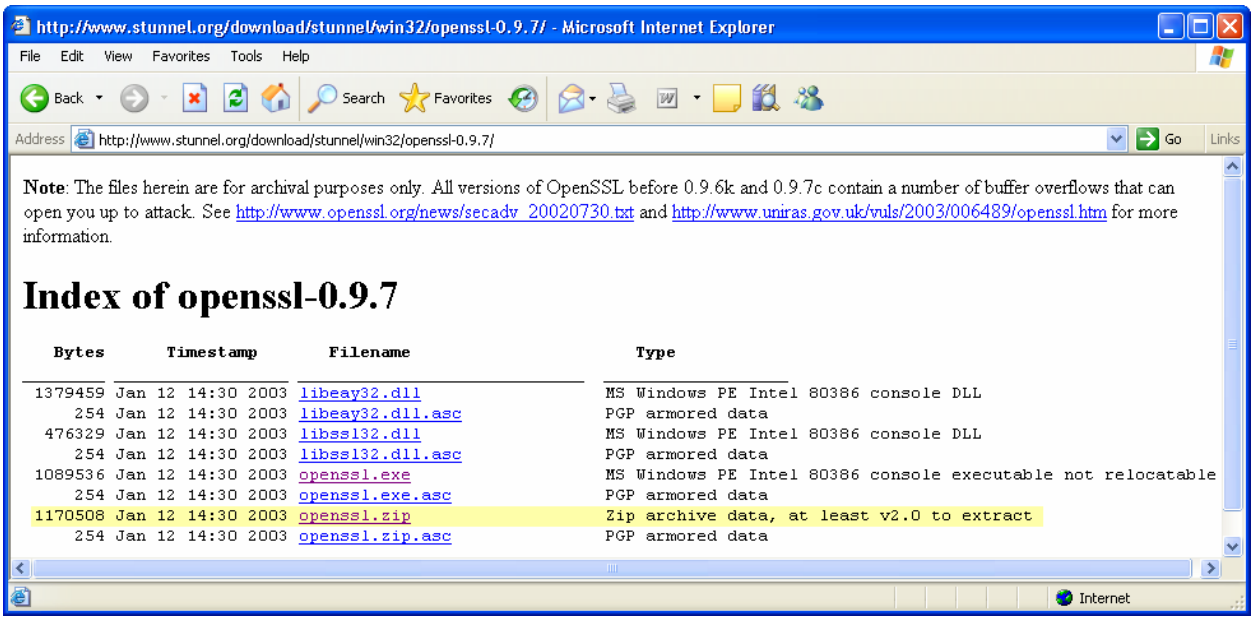

Figure 5.1. Openssl.exe

3. click **openssl.zip**, displaying Figure 5.2,

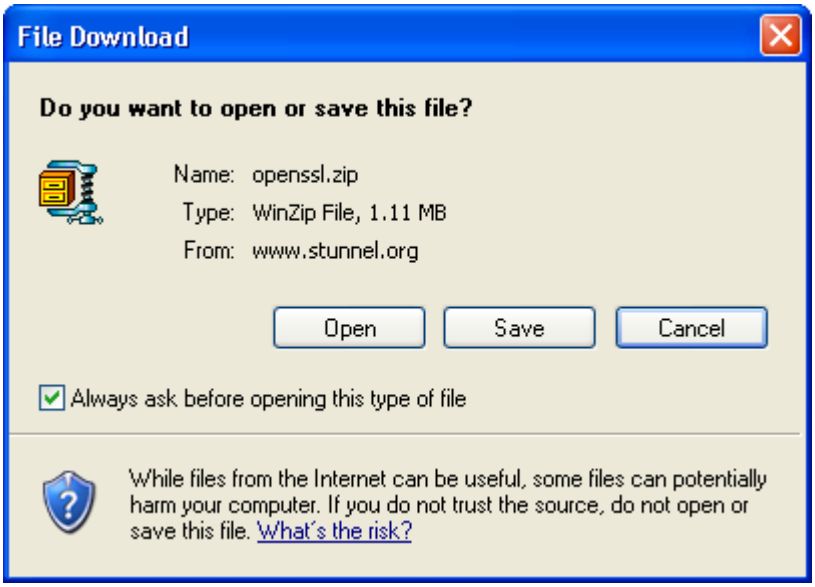

Figure 5.2. Openssl File Download

4. select **Open**, displaying Figure 5.3,

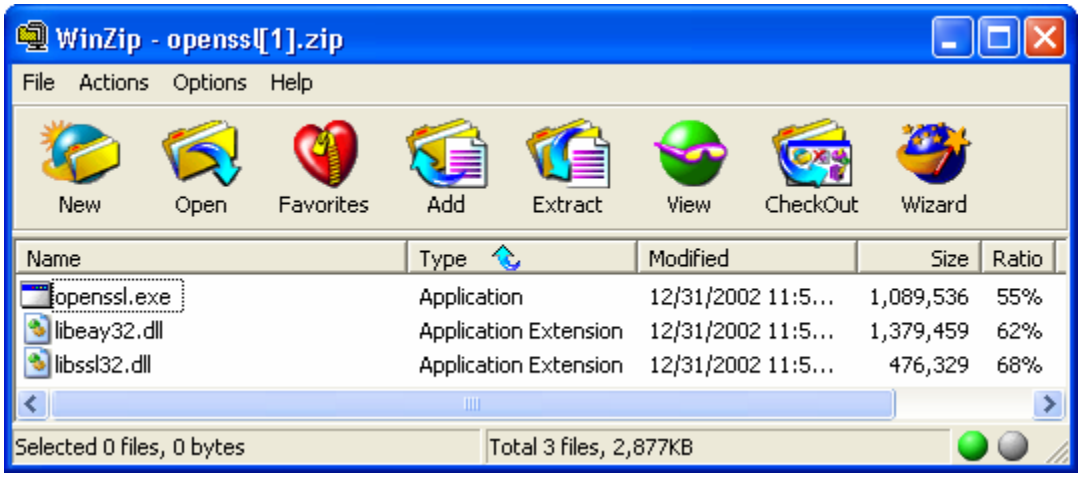

Figure 5.3. WinZip Openssl

5. select **Extract** displaying Figure 5.4, and

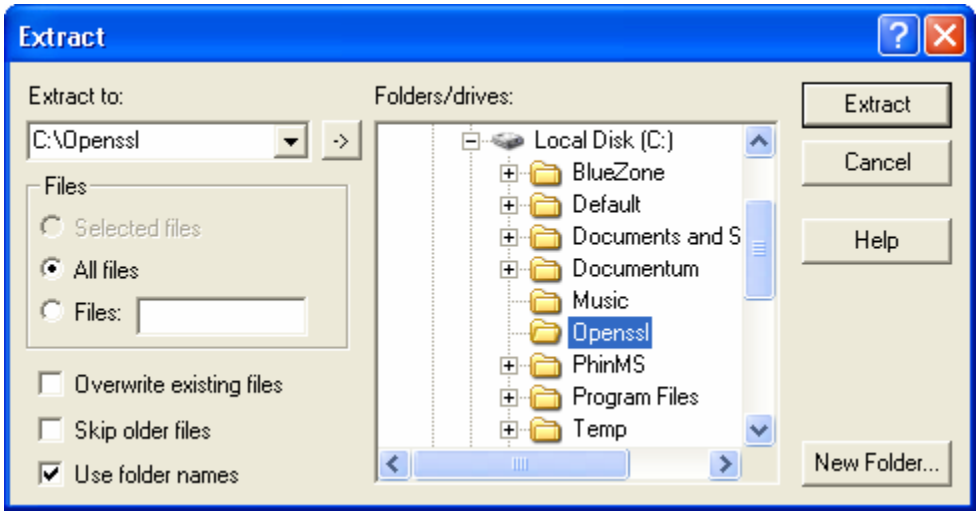

Figure 5.4. Extract Files

6. navigate to the **Openssl** folder, click **Extract**, close window.

Note: The following four files are needed to run Openssl shown in Figure 5.5:

- libeay32.dll,
- libssl32.dll,
- openssl.exe, and
- openssl.conf.

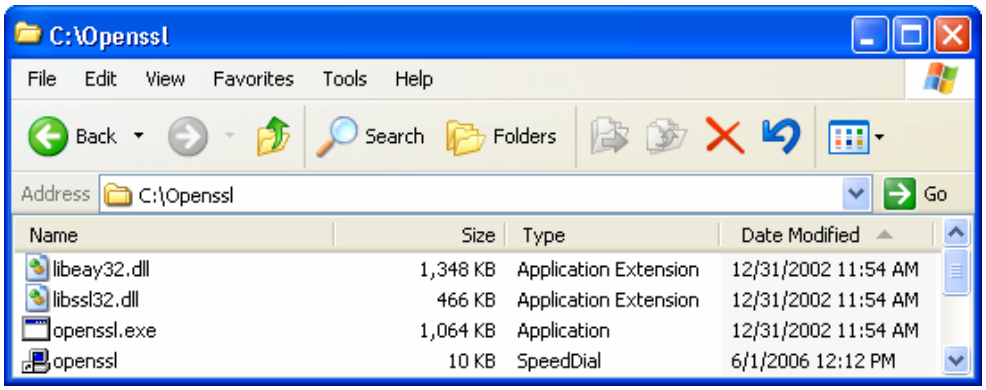

Figure 5.5. Openssl Files

The first three files libeay32.dll, libssl.dll, and open.exe are automatically extracted from the WinZip file. The fourth, openssl needs to be downloaded from PHINMS FTP site. Contact the PHIN Help Desk for assistance phintech@cdc.gov.

5.2 Create Self-Signed Certificates

Complete the following steps to create a Self-Signed Certificates:

1. navigate to **C:\openssl**, double click on **openssl.exe** displaying Figure 5.6,

Figure 5.6. Openssl

2. type req -new -x509 -days 365 -nodes -config openssl.cnf -out c:\openssl\renamecsr.pem -keyout c:\openssl\renamekey.pem, select Enter displaying Figure 5.7,

Note: Replace both "rename" in step two with a unique file name. An example would be phinmscsr.pem and phinmskey.pem. Do not replace csr.pem or key.pem.

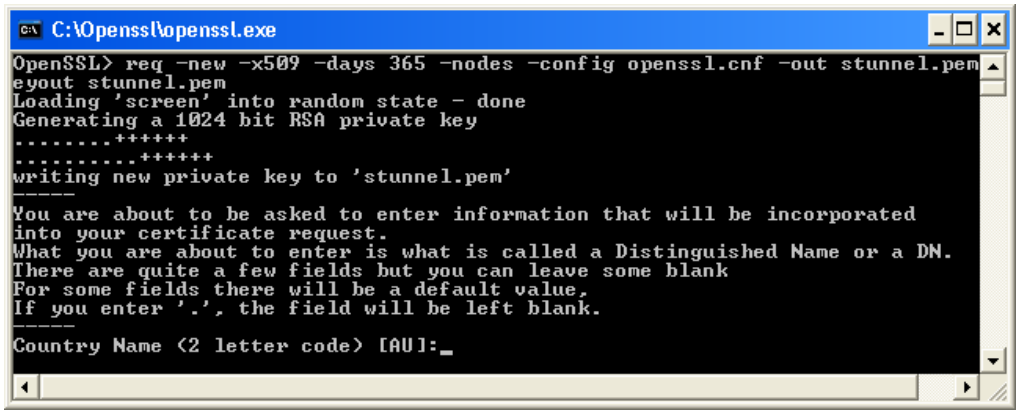

Figure 5.7. Distinguished Name Prompts

3. assign the Distinguished Name (DN) Fields command prompts with information uniquely identifying the Self-Signed Certificates using the examples in Table 1 as a guideline displaying Figure 5.8, and

Note: The DN fields will be incorporated into the Self-Signed Certificates request. The prompts allow blank fields but it is highly recommended to complete all the fields. This will uniquely identify the Self-Signed Certificates.

FIELDS	EXAMPLES
Country Name:	PL, UK, US, CA
State or Province Name:	Illinois, Ontario
Locality:	Chicago, Toronto
Organization Name:	Bill's Meats, Acme Anvils
Organizational Unit Name:	Ecommerce Division
Common Name (FQDN)	www.example.com
Email address	test@yahoo.com

Table 1. Distinguished Name Fields Examples

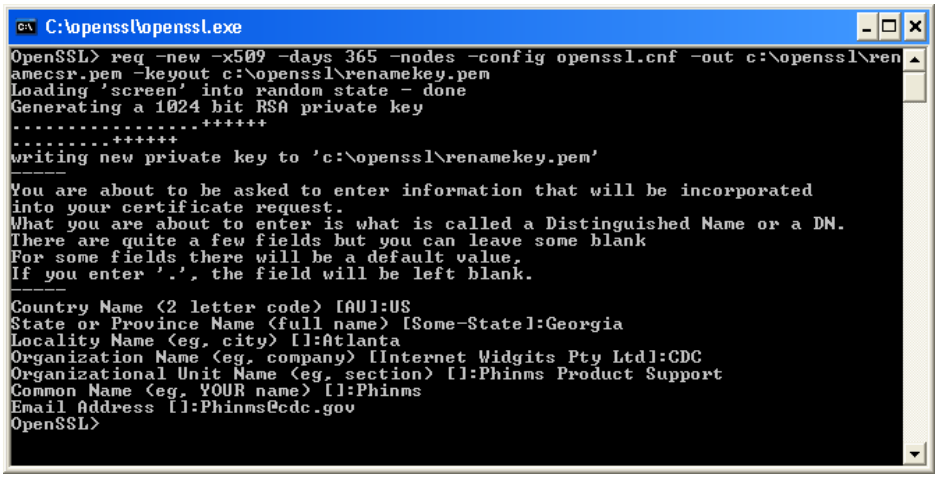

Figure 5.8. Distinguished Name Fields

4. close the window.

The new Self-Signed Certificates should be in the C:\openssl folder as shown in Figure 5.9.

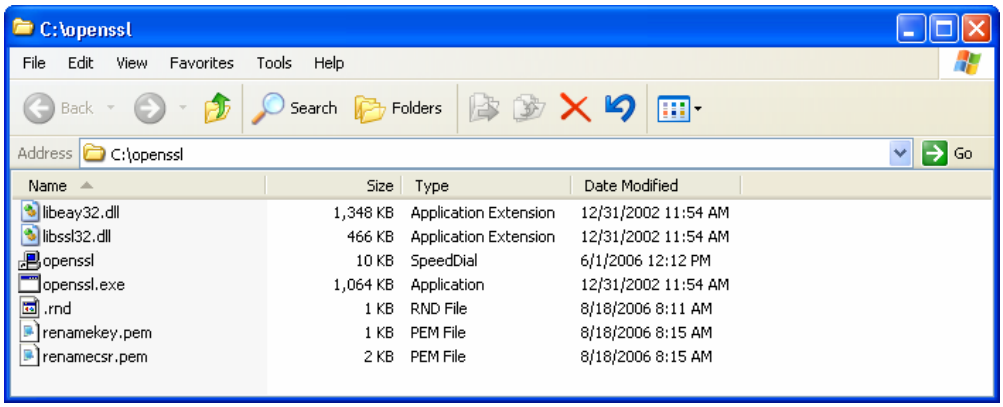

Figure 5.9. Self-Signed Certificates

5.3 Configure Servers

Complete the following steps to configure secure communications between the two servers using Stunnel:

1. copy the two (2) **Self-Signed Certificates** created,
2. select **Start > Programs > Stunnel, Edit Stunnel.conf** displaying the left screen in Figure 5.10,

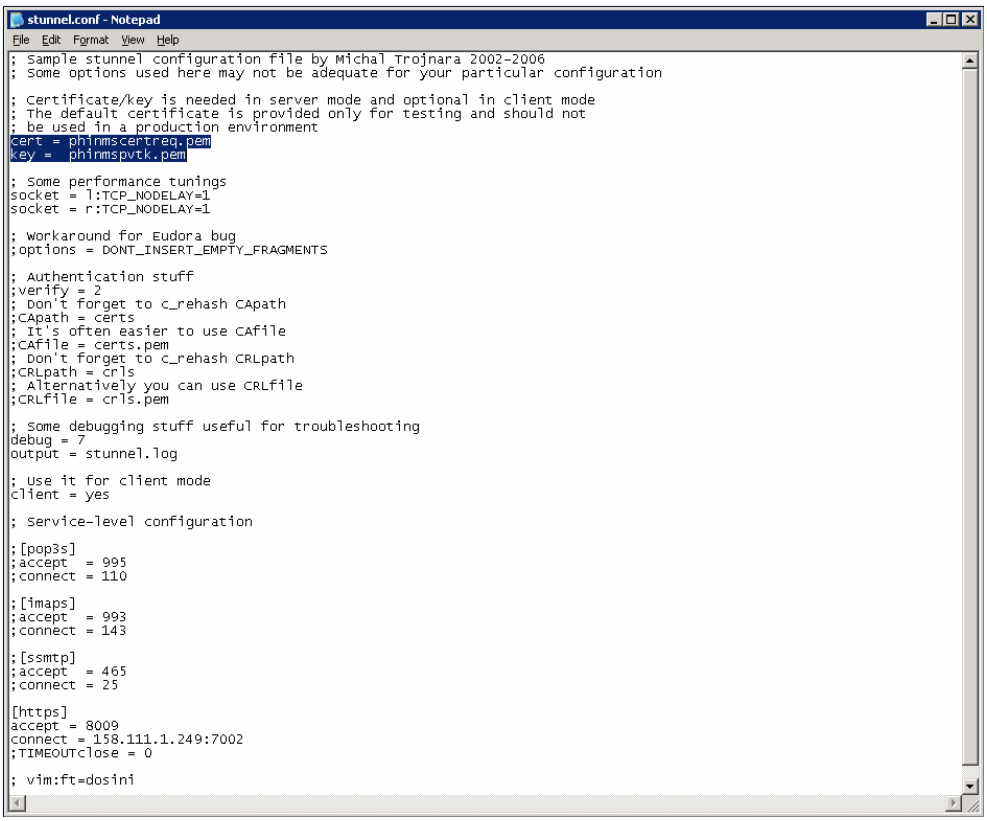

Figure 5.10. Stunnel Configuration File

3. paste the two (2) **Self-Signed Certificates** into the Stunnel.conf file on the lines highlighted in Figure 5.10,

Note: Ensure the Self-Signed Certificates are identified as key or cert in the name which helps in configuring Stunnel.conf file.

4. close window displaying Figure 5.11,

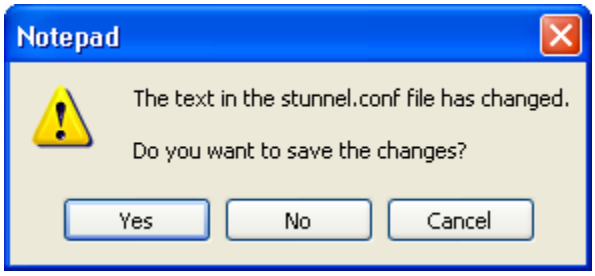

Figure 5.11. Save Stunnel.conf File

5. select **Yes**,
6. select **Start > Programs > Stunnel, Service stop**, and
7. select **Start > Programs > Stunnel, Service start** on both servers.