A MITEL
PRODUCT
GUIDE

OpenScape Deployment Service V10

HTTPS Configuration Guide

Service Documentation

Service Documentation

10/2019

A31003-S23A0-S100-01-76A9

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively "Unify") or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

History of Changes

Version	Date	Changes	Author(s)

Table of Content

1 INTRODUCTION

1.1 Scope

This manual is intended for DLS and OpenStage Test Teams, Service Technician and Customers with interest in HTTPS Deployment.

The manual describes how the user should configure the HTTPS Server and DLS in order to use HTTPS Deployment. Sections 2 and 3 focus on HTTPS configuration in a Microsoft Windows environment.Section 4 of this guide embraces the HTTPS configuration for a SUSE Linux based server / OpenSUSE environment.

2 Configuration

2.1 Software Requirements

– ASP 2.0 OR PHP

– IIS 5.1/6.0/7.0 OR xampp (Apache HTTP Server)

– For IIS Application Servers, Microsoft .NET Framework Version 2.0 (see [9] for download)

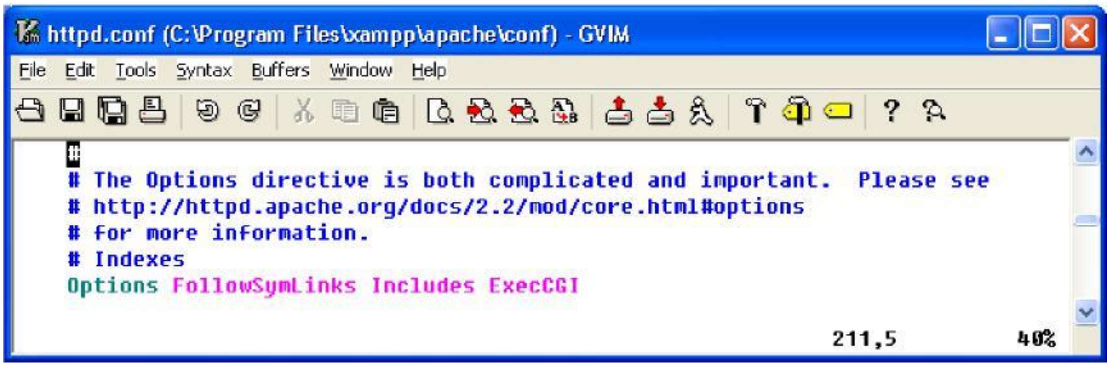
– Service Packs: download and install available service packs, it is recommended to update the Windows OS using Microsoft Update to the current security patch level.

2.2 HTTPS Server

The following subsections describe how the HTTP Server should be prepared for HTTPS Donwloads in DLS. Only the XAMPP Apache HTTP Server, IIS 5.1, IIS 6.0 and IIS 7 are tested with DLS.

2.2.1 Apache 2.2.3 (XAMPP)

1. Download and install XAMPP [1]
2. See the instructions to make XAMPP secure in [6]
3. You can either enable or disable directory listing. This behavior can be configured from <xampp>\apache\conf\httpd.conf. The Indexes directive must be added to the Options keyword if directory listing is desired (e.g., *Options* FollowSymLinks Includes ExecCGI *Indexes*).


httpd.conf (C:\Program Files\xampp\apache\conf) - GVIM
File Edit Tools Syntax Buffers Window Help
211,5
40%

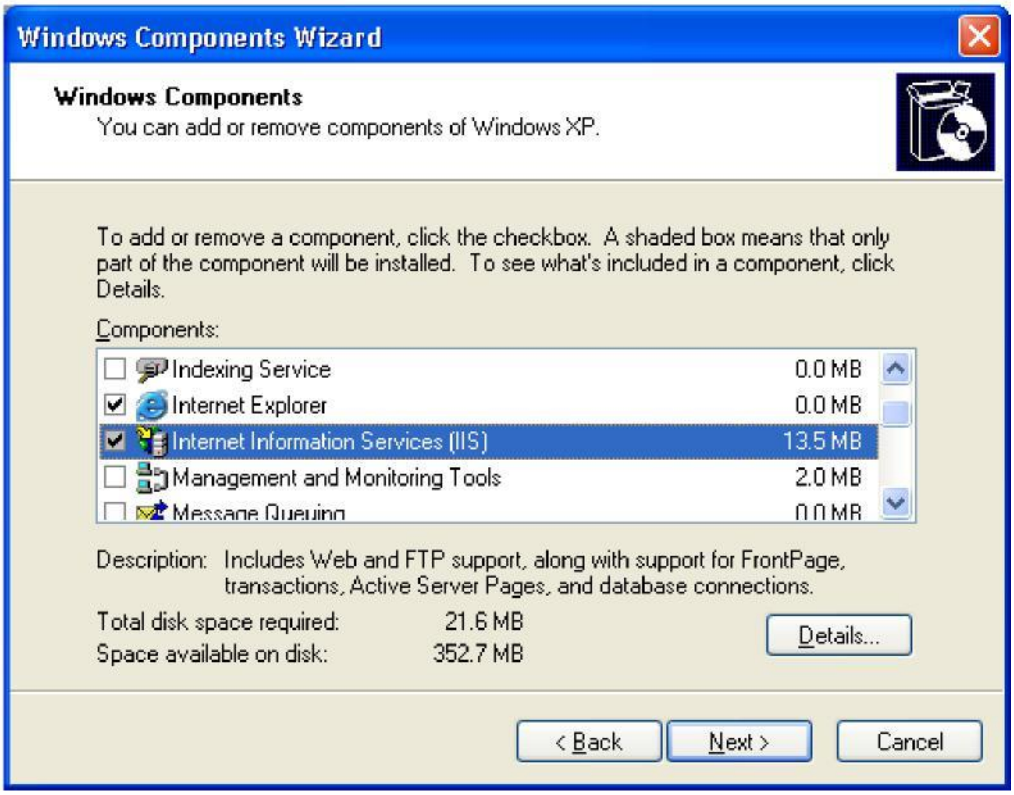
```
#
# The Options directive is both complicated and important.  Please see
# http://httpd.apache.org/docs/2.2/mod/core.html#options
# for more information.
# Indexes
Options FollowSymLinks Includes ExecCGI
```

Figure 1 Apache Directory Listing (disabled)

4. For Apache HTTPS Server only, if directory listing is disabled, the dls directory lister script (PHP) must be added to the HTTPS Base defined in DLS (see sections 3.1 and 3.2)

2.2.2 IIS 5.1

1. Install IIS from „Add/Remove Programs“ 🖎✉ “Add Remove Windows Components”. In the Windows Component Wizard, select Internet Information Services (IIS) and follow the instructions.



Windows Components Wizard

Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☐ Indexing Service 0.0 MB
☑ Internet Explorer 0.0 MB
☑ Internet Information Services (IIS) 13.5 MB
☐ Management and Monitoring Tools 2.0 MB
☐ Message Queuing 0.0 MB

Description: Includes Web and FTP support, along with support for FrontPage, transactions, Active Server Pages, and database connections.

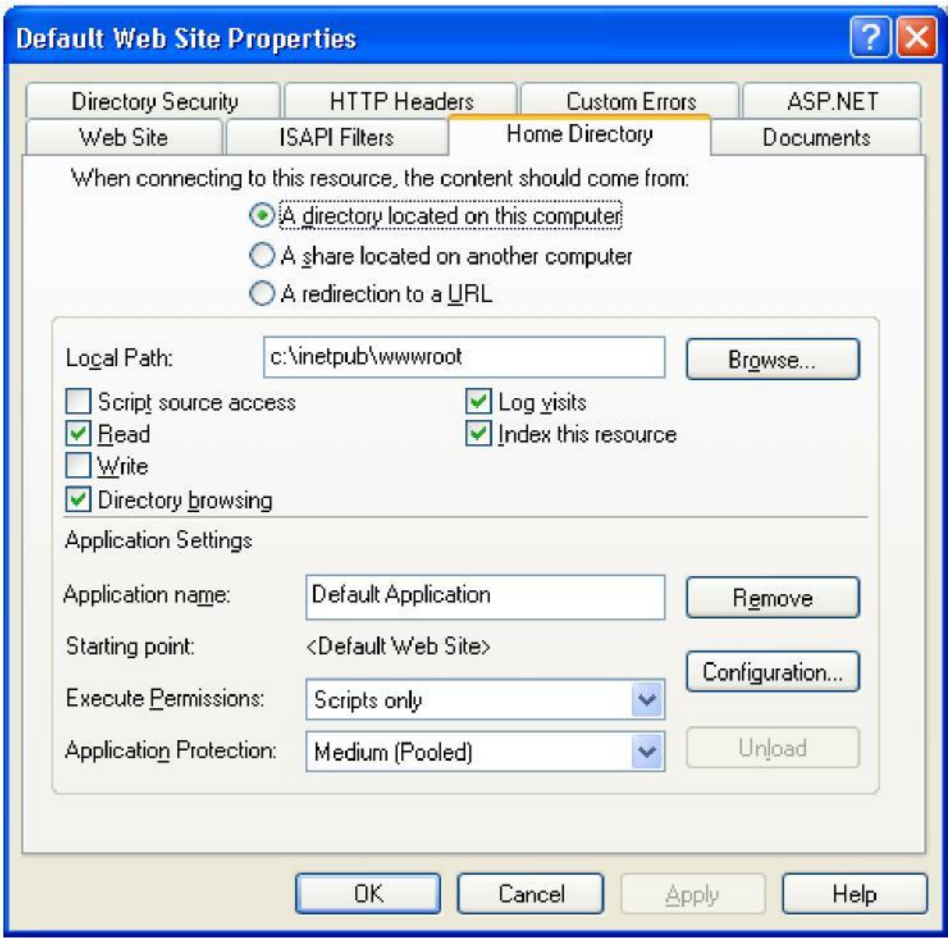
Total disk space required: 21.6 MB
Space available on disk: 352.7 MB

Figure 2 IIS installation

2. See Security configuration section in [7].

3. From the Control Panel, go to “Administrative Tools” and then “Internet Information Services”.

4. Configure your Web Site as follows:



When connecting to this resource, the content should come from:

● A directory located on this computer
○ A share located on another computer
○ A redirection to a URL

Local Path: c:\inetpub\wwwroot

□ Script source access
☑ Read
□ Write
☑ Directory browsing
☑ Log visits
☑ Index this resource

Application Settings

Application name: Default Application

Starting point: <Default Web Site>

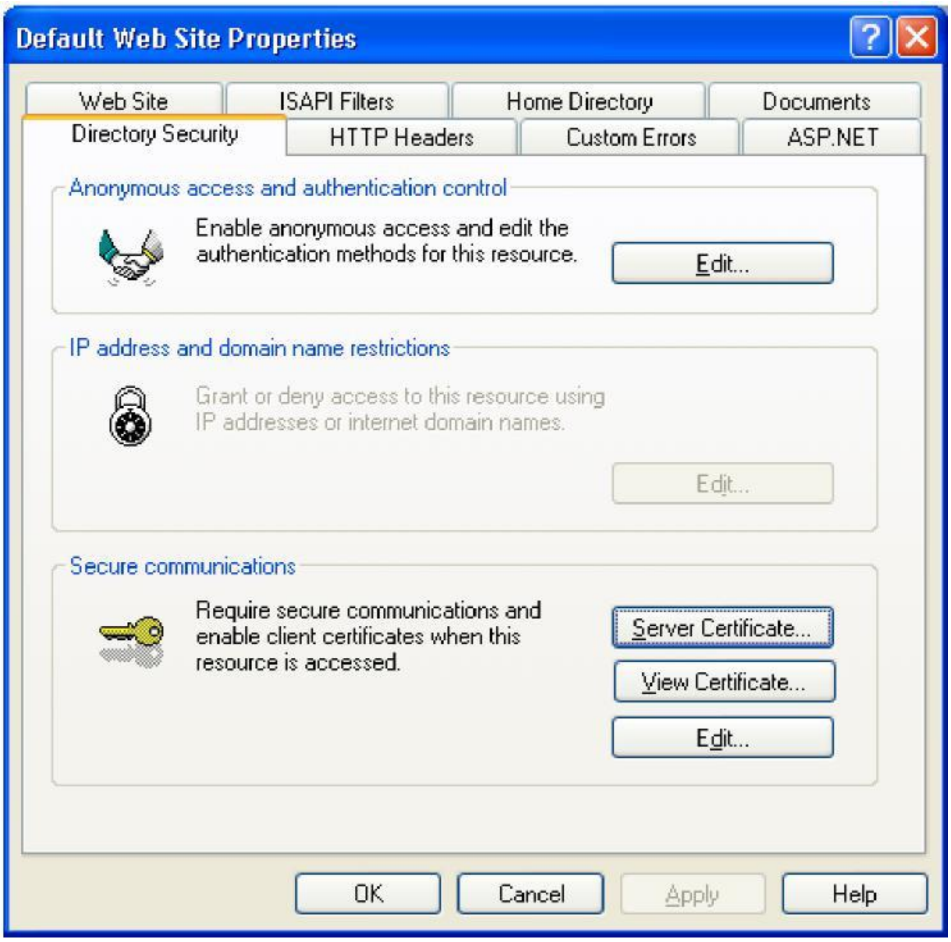
Execute Permissions: Scripts only

Application Protection: Medium (Pooled)

Figure 3 IIS Configuration

5. Please note that, you can enable or disable the Directory browsing and Indexing of the resource.

6. In the Directory Security tab create a Server Sertificate using the Web Server Certificate Wizard. To create a Certificate you can donwload IIS Resources [2] and use SelfSSL (for details see Reference [3]).



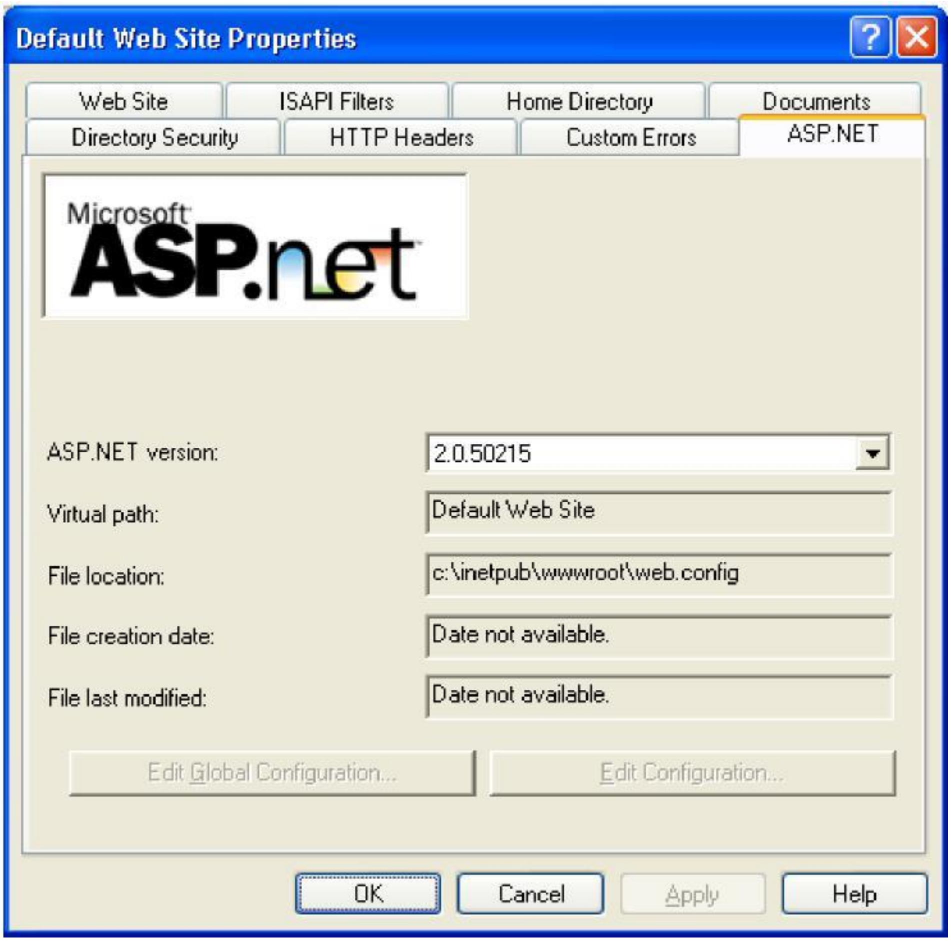
Enable anonymous access and edit the authentication methods for this resource.

Grant or deny access to this resource using IP addresses or internet domain names.

Require secure communications and enable client certificates when this resource is accessed.

Figure 4 IIS Server Certificate creation

7. Copy the dls directory lister script (ASP) to the HTTPS Base defined in DLS (see sections 3.1 and 3.2)
8. Make sure that you are using ASP 2.0. Check this in the ASP.NET tab:



ASP.NET version: 2.0.50215

Virtual path: Default Web Site

File location: c:\inetpub\wwwroot\web.config

File creation date: Date not available.

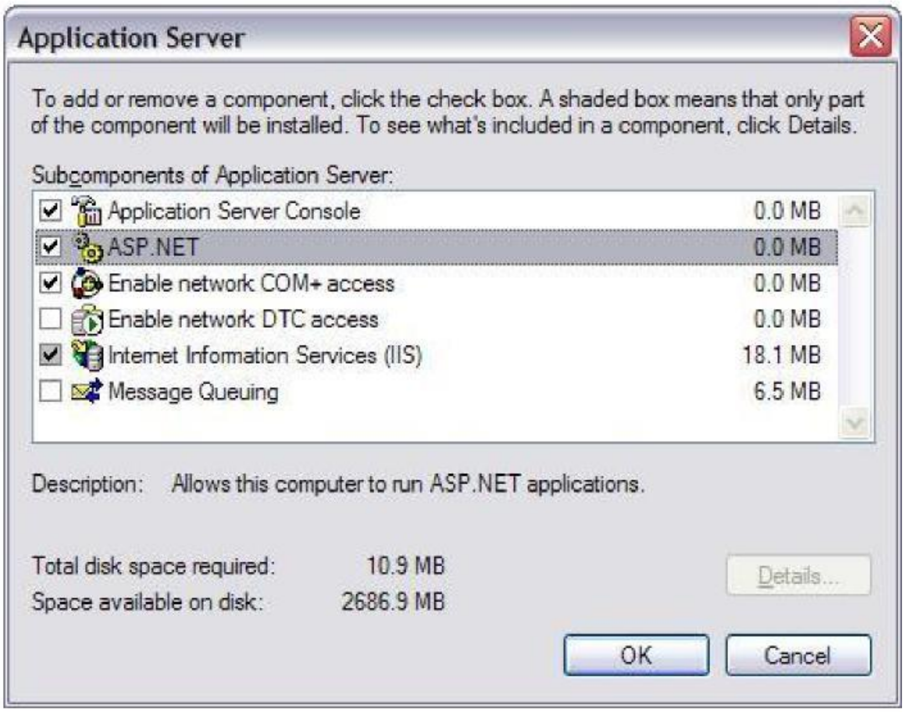
File last modified: Date not available.

Figure 5 IIS ASP.NET version

9. Check in DLS if you can access the HTTPS Server, and create an image.

2.2.3 IIS 6.0

1. Install IIS 6.0 from Add/Remove Programs ☝✉ Add/Remove Windows Components ☝✉ Application Server (see [8] for details on how to install ASP.NET). Make sure that you select ASP.NET in the Application Server section (see Figure 6).



Application Server

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Application Server:

☑ Application Server Console	0.0 MB
☑ ASP.NET	0.0 MB
☑ Enable network COM+ access	0.0 MB
□ Enable network DTC access	0.0 MB
☑ Internet Information Services (IIS)	18.1 MB
□ Message Queuing	6.5 MB

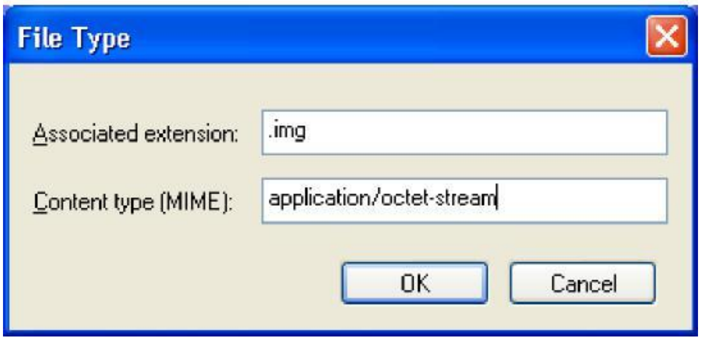
Description: Allows this computer to run ASP.NET applications.

Total disk space required: 10.9 MB

Space available on disk: 2686.9 MB

Figure 6 - Select ASP.NET and IIS

2. Configure the IIS Server (see Figure 3)
3. See Security configuration section in [7].
4. Create Server Certificate (see Figure 4). To create a Certificate you can donwload IIS Resources [2] and use SelfSSL (for details see Reference [3]).
5. In the IIS Manager, go to Web Service Extensions, and make sure that Active Server Pages is set to “Allow”, and that its version is ASP 2.0.
6. Right-click on the Web-Sites Tree-Node, and click Properties.
7. Go to the “HTTP Headers” Tab, and click on Mime Types.
8. Make sure that File-extensions to be downloaded are supported (e.g., .img). If the .img extension is not in the list defined the extension as application/octet-stream



File Type

Associated extension: .img

Content type (MIME): application/octet-stream

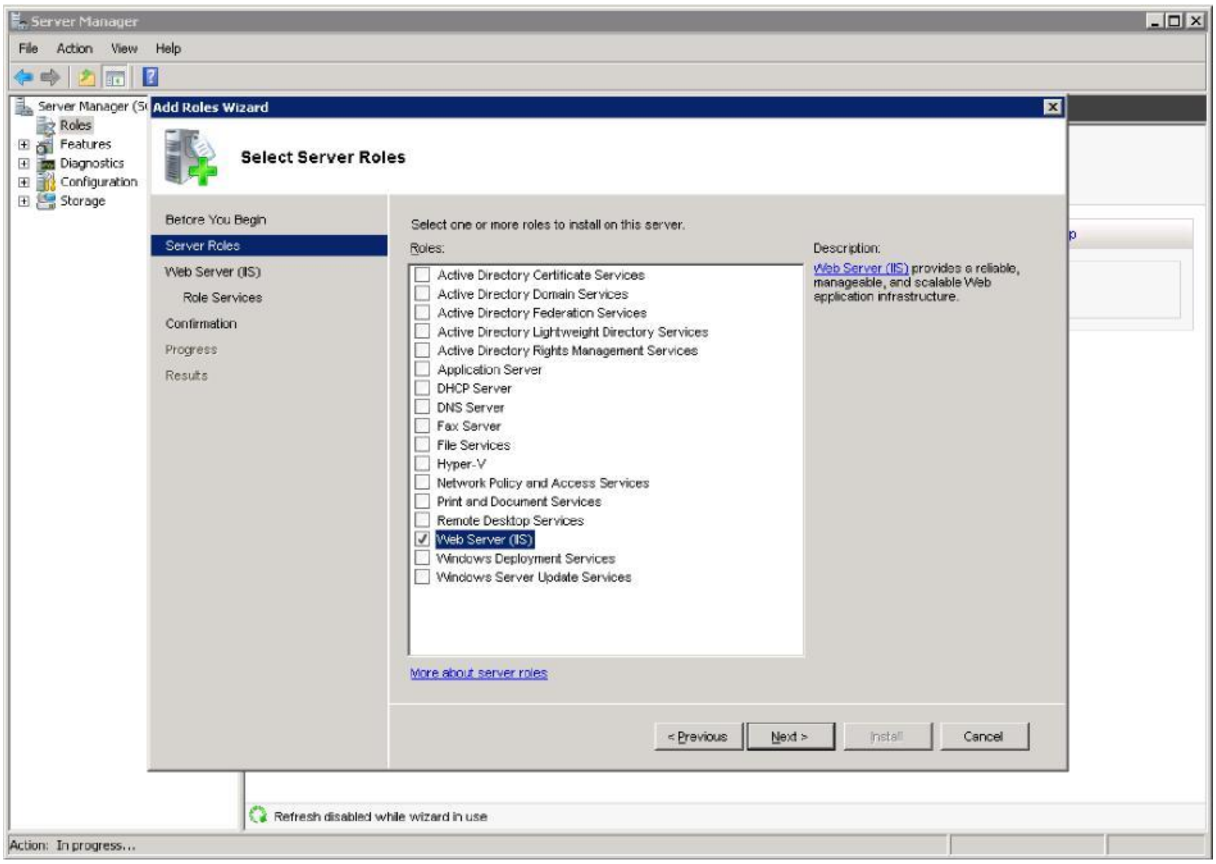
Figure 7 defining the img extension

9. Copy the dls directory lister script (ASP) under the HTTPS Server URL defined in DLS (see sections 3.1 and 3.2). Please note that you cannot access the contents of the IIS Server without this script (even if directory listing is enabled).
10. Check in the browser if the URL of the software image and the dls directory lister is accessible. If a 404 (The page is not found) error is given, you should check your

HTTP Server configuration. Neither DLS nor the phone will be able to access the image.

2.2.4 IIS 7.0

1. On Windows Versions which support IIS 7 (like Windows 2008 R2) Install IIS 7.0 from Start 📪⌧ Administrative Tools 📪⌧ Server Manager. Select “Roles” in the tree and select “Add Roles” in the Right Mouse Popup Menu. The “Add Roles Wizard” Opens. Click Next to reach following screen where you select “Web Server (IIS)”



Select Server Roles

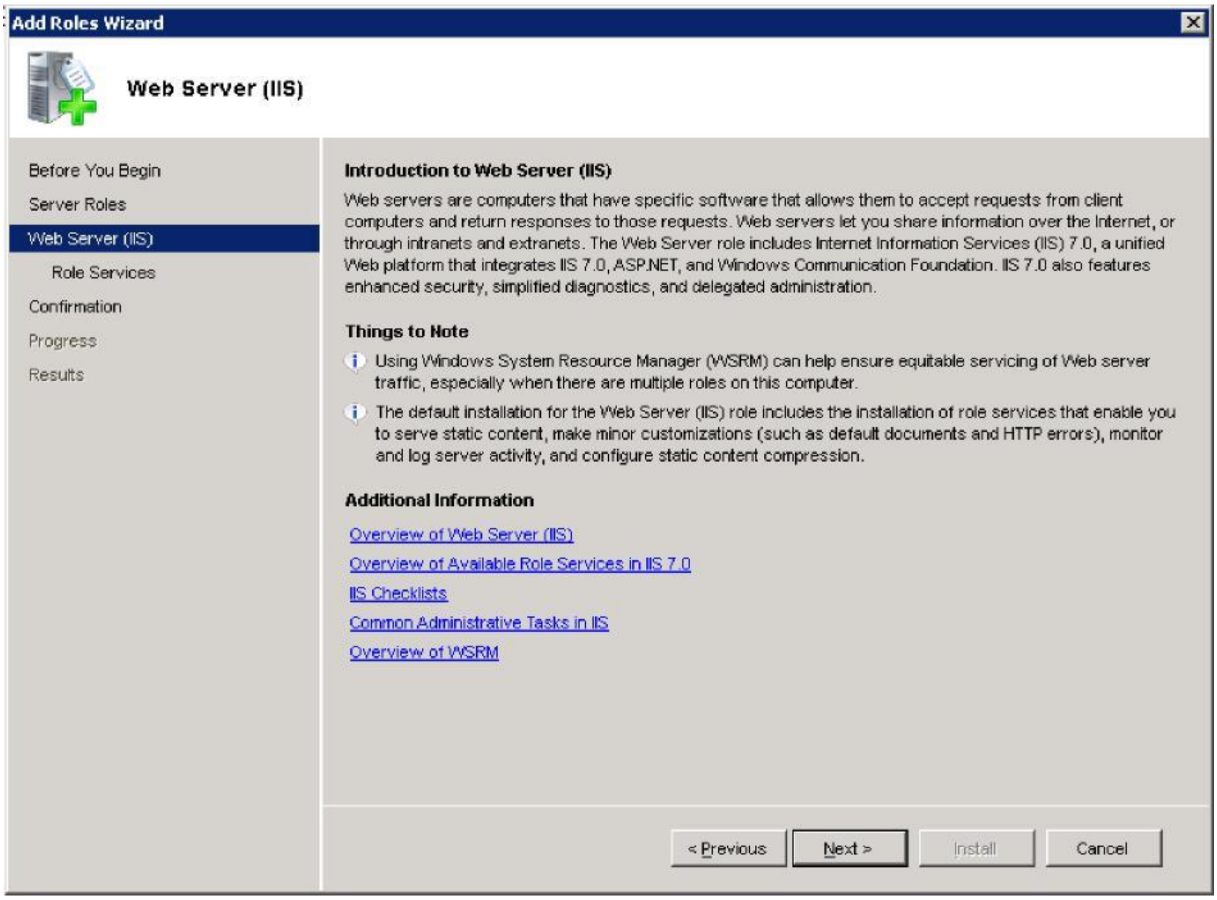
Select one or more roles to install on this server.

Roles:

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Desktop Services
- ☑ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description:
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Click Next:



Introduction to Web Server (IIS)

Web servers are computers that have specific software that allows them to accept requests from client computers and return responses to those requests. Web servers let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 7.0, a unified Web platform that integrates IIS 7.0, ASP.NET, and Windows Communication Foundation. IIS 7.0 also features enhanced security, simplified diagnostics, and delegated administration.

Things to Note

Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic, especially when there are multiple roles on this computer.

The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

Additional Information

Overview of Web Server (IIS)

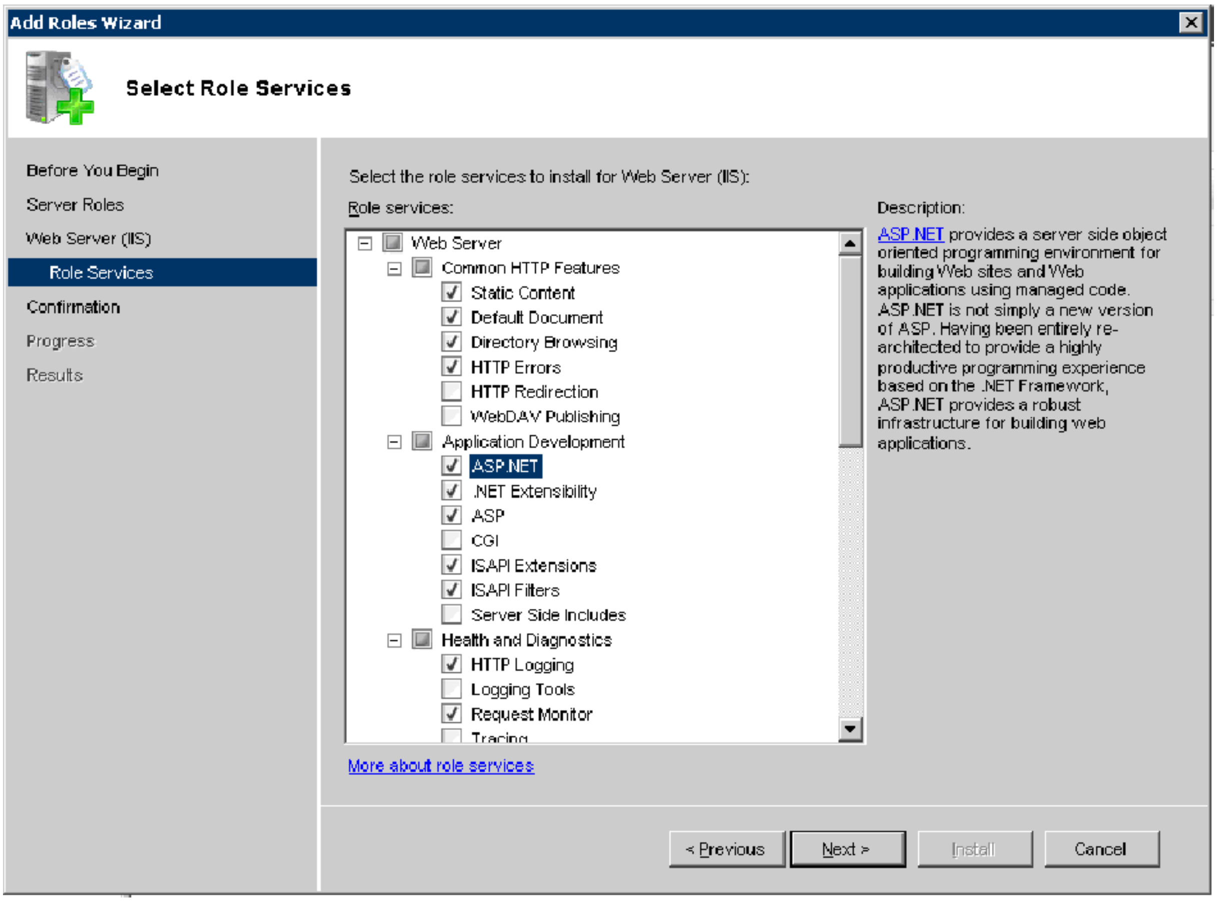
Overview of Available Role Services in IIS 7.0

IIS Checklists

Common Administrative Tasks in IIS

Overview of WSRM

Click Next



Select the role services to install for Web Server (IIS):

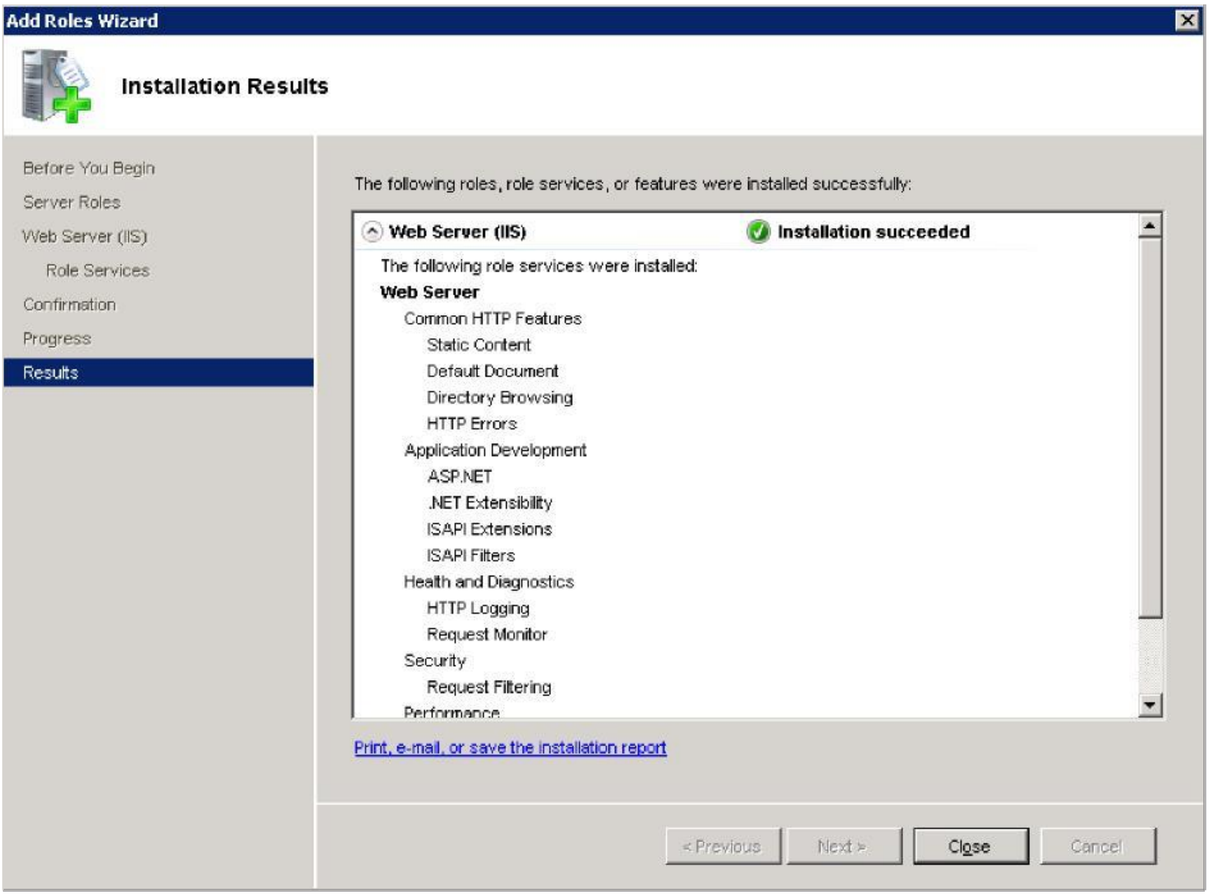
Role services:

- Web Server
  - Common HTTP Features
    - ☑ Static Content
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - □ HTTP Redirection
    - □ WebDAV Publishing
  - Application Development
    - ☑ ASP.NET
    - ☑ .NET Extensibility
    - ☑ ASP
    - □ CGI
    - ☑ ISAPI Extensions
    - ☑ ISAPI Filters
    - □ Server Side Includes
  - Health and Diagnostics
    - ☑ HTTP Logging
    - □ Logging Tools
    - ☑ Request Monitor
    - □ Tracing

Description:

ASP.NET provides a server side object oriented programming environment for building Web sites and Web applications using managed code. ASP.NET is not simply a new version of ASP. Having been entirely re-architected to provide a highly productive programming experience based on the .NET Framework, ASP.NET provides a robust infrastructure for building web applications.

Keep the defaults and select “ASP .NET” and “ASP” in addition.
Click Next and Install on that screen.



The following roles, role services, or features were installed successfully:

Web Server (IIS) ✓ Installation succeeded

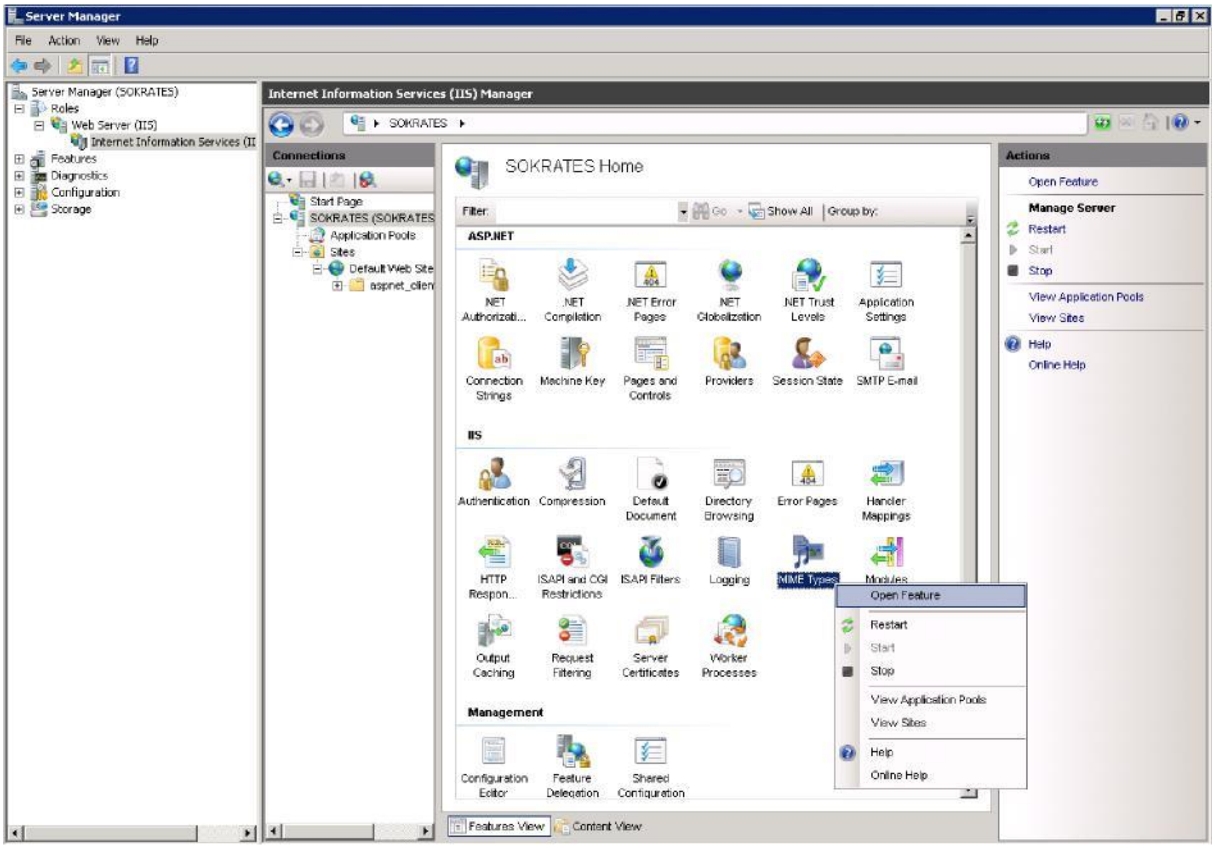
The following role services were installed:

Web Server

- Common HTTP Features
  - Static Content
  - Default Document
  - Directory Browsing
  - HTTP Errors
- Application Development
  - ASP.NET
  - .NET Extensibility
  - ISAPI Extensions
  - ISAPI Filters
- Health and Diagnostics
  - HTTP Logging
  - Request Monitor
- Security
  - Request Filtering
- Performance

2. Add a mime type

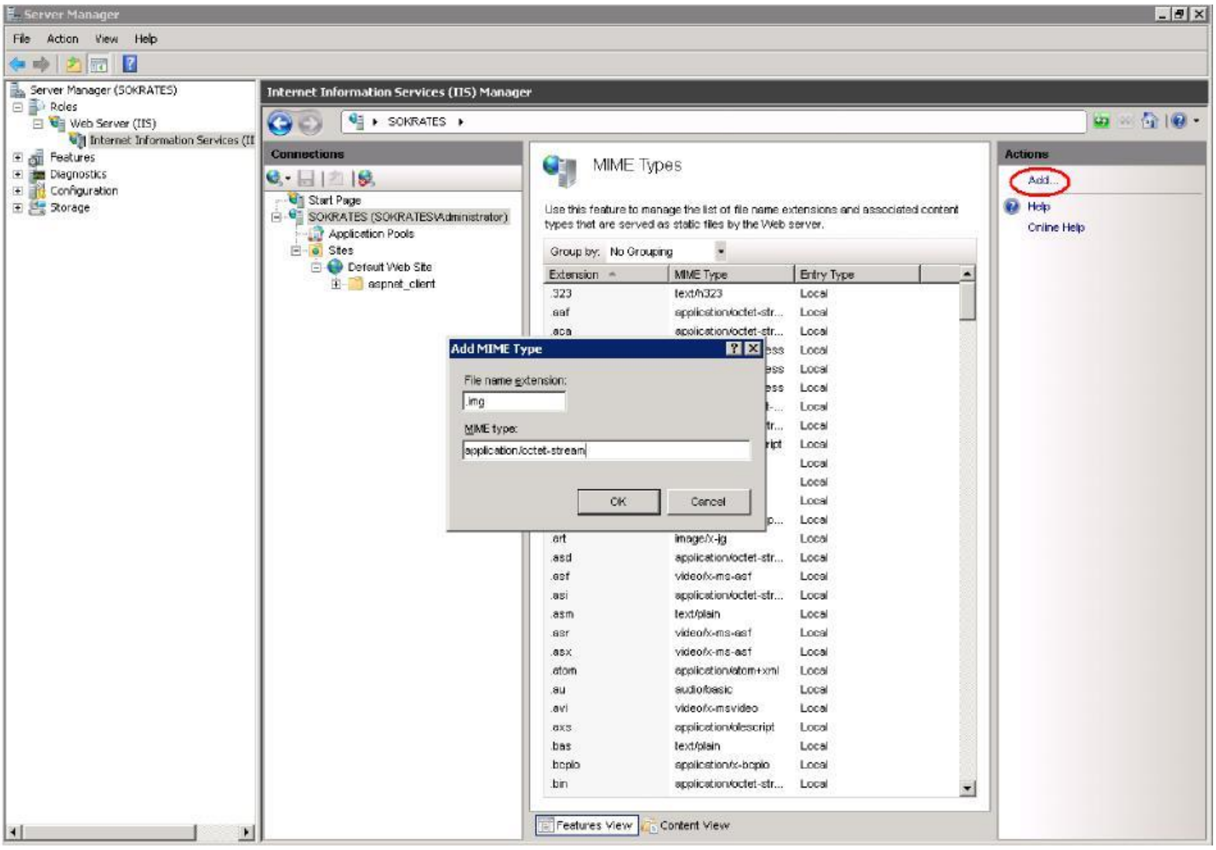
Click on “Internet Information Services (IIS) Manager ” below Roles->Web Server (IIS) in the Server Manager, Select the entry below “Start Page” on the “Internet Information Services (IIS) Manager” Screen named as the system’s hostname, “SOKRATES” in the example below, Right Click “Mime Type” and “Open Feature” in that popup:



Click “Add” on the screen that opens and add following mime type:

Extension: .img

MIME type: application/octet-stream



MIME Types

Use this feature to manage the list of file name extensions and associated content types that are served as static files by the Web server.

Group by: No Grouping

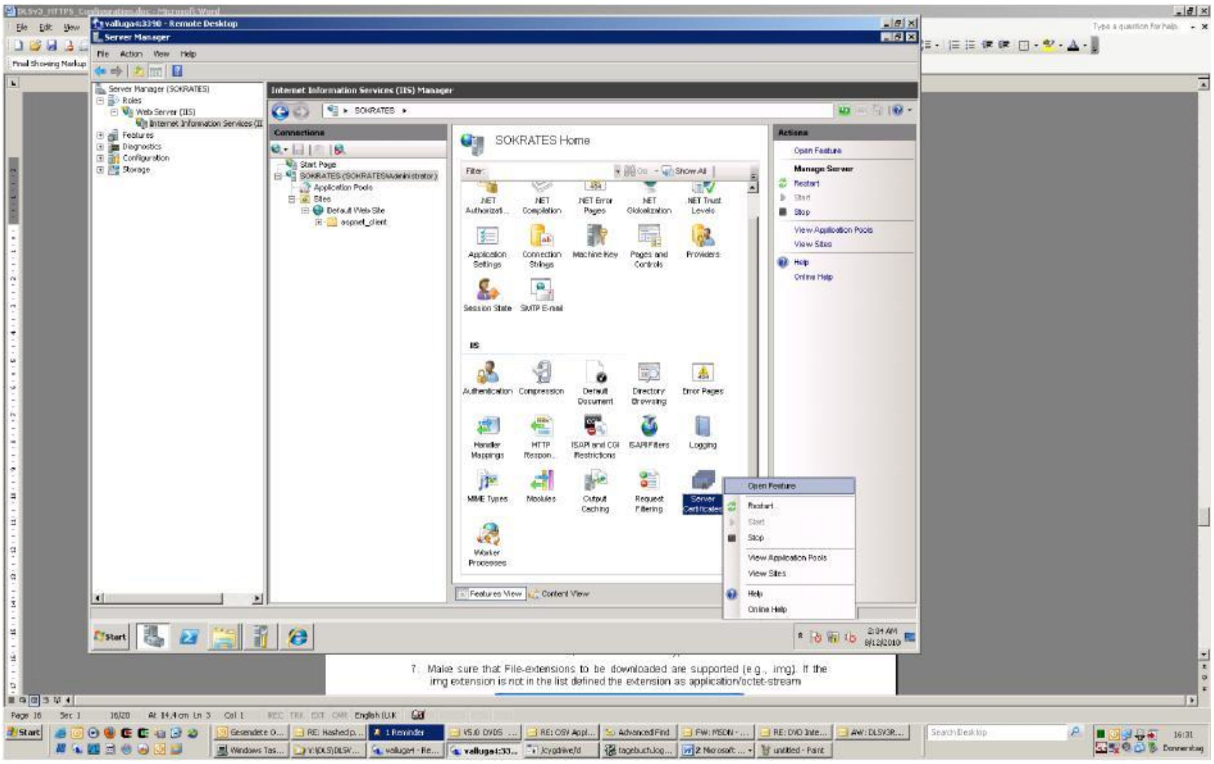
Extension	MIME Type	Entry Type
.323	text/h323	Local
.aaf	application/octet-str...	Local
.aca	application/octet-str...	Local
	...ess	Local
	...ess	Local
	...ess	Local
	...l-...	Local
	...tr...	Local
	...ript	Local
		Local
		Local
		Local
	...p...	Local
.art	image/x-jg	Local
.asd	application/octet-str...	Local
.asf	video/x-ms-asf	Local
.asi	application/octet-str...	Local
.asm	text/plain	Local
.asr	video/x-ms-asf	Local
.asx	video/x-ms-asf	Local
.atom	application/atom+xml	Local
.au	audio/basic	Local
.avi	video/x-msvideo	Local
.axs	application/olescript	Local
.bas	text/plain	Local
.bcpio	application/x-bcpio	Local
.bin	application/octet-str...	Local

Add MIME Type

File name extension: .img

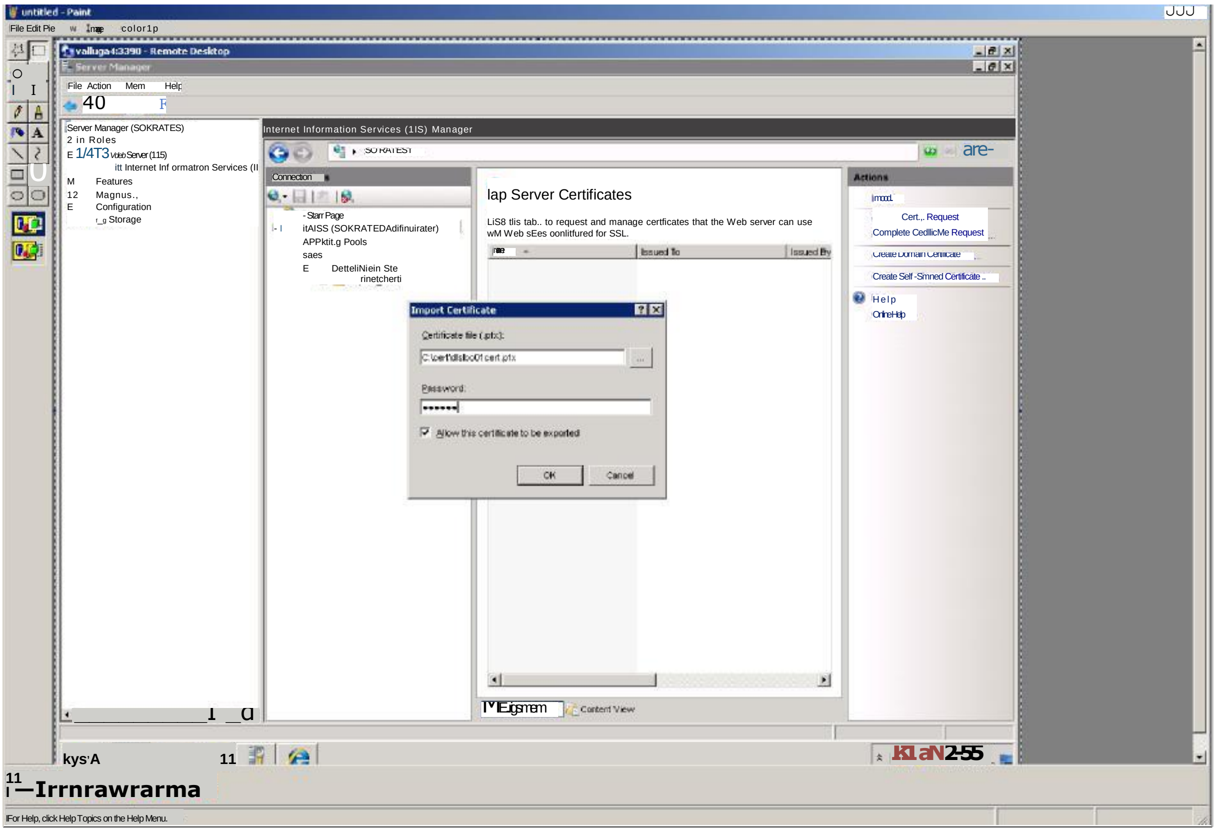
MIME type: application/octet-stream

3. Similar as above open “Server Certificates” -> “Open Feature”



7. Make sure that File-extensions to be downloaded are supported (e.g., .img). If the .img extension is not in the list defined the extension as application/octet-stream

Click Import on the next screen and import a server certificate and password (.pfx) extension:



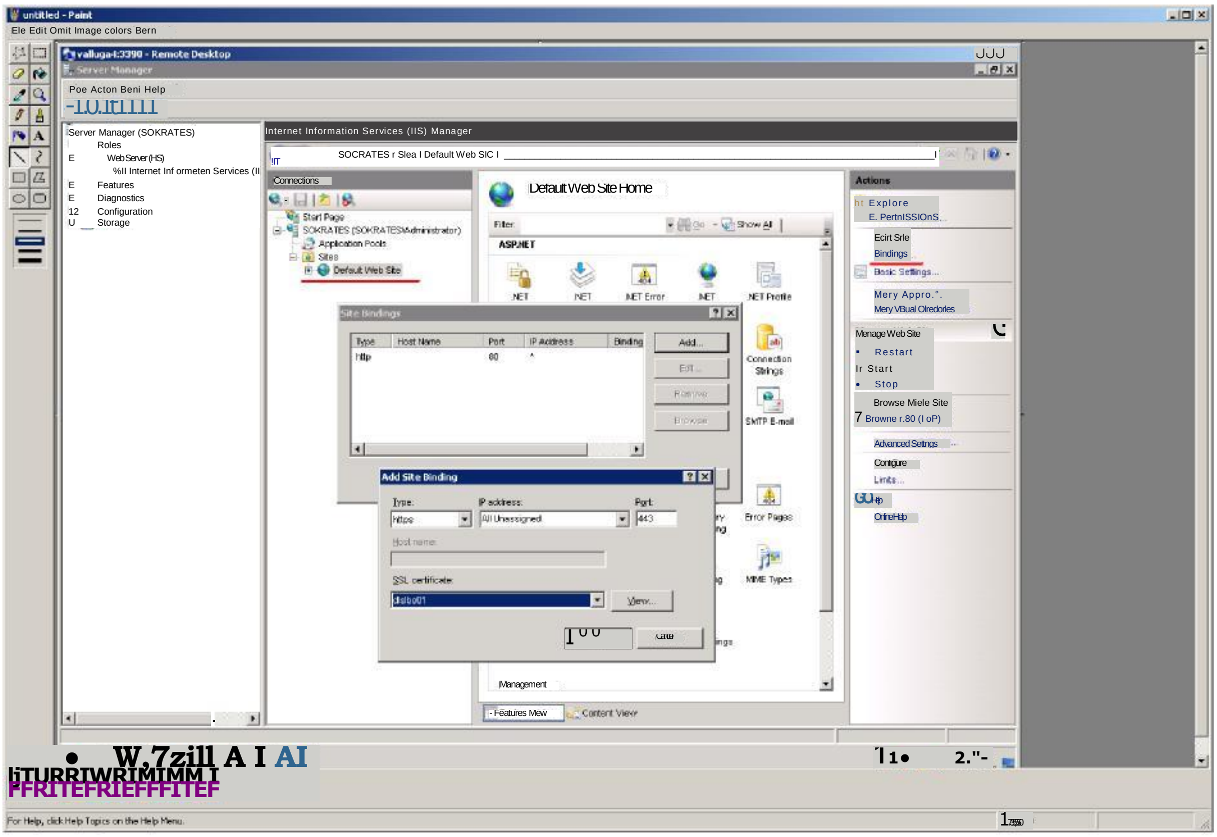
Import Certificate

Certificate file (.pfx): C:\cert\dlsbo01cert.pfx

Password: ••••••

☑ Allow this certificate to be exported

Select the "Default Web Site", click on "Bindings" and add https providing port



Site Bindings

Type	Host Name	Port	IP Address	Binding
http		80	*	

Add Site Binding

Type: https

IP address: All Unassigned

Port: 443

Host name:

SSL certificate: dlsbo01

and certificate:

4. Copy the dls directory lister script (ASP) under the HTTPS Server URL defined in DLS (see sections 3.1 and 3.2). Please note that you cannot access the contents of the IIS Server without this script (even if directory listing is enabled).
5. Check in the browser if the URL of the software image and the dls directory lister is accessible. If a 404 (The page is not found) error is given, you should check your HTTP Server configuration. Neither DLS nor the phone will be able to access the image.

2.3 DLS

Configure the HTTPS Server from Administration 📫🖂 Server Configuration 📫🖂 HTTPS Server Configuration. Provide the HTTPS Server URL like https://<url>/<path>. Non secure paths are also allowed if respectively configured on the other end. For more information on configuring DLS, please consult DLS's documentation and also chapter 3.5 in this document.

3 Common Problems

3.1 Where is the PHP/ASP Script?

The PHP and ASP scripts can be found in the DLS CD under the tools directory. The scripts are named:

– dls_directory_reader.asp –

dls_directory_reader.php

3.2 Where should the PHP/ASP Script from the CD copied to?

The script must be copied under the root directory defined as "HTTPS Server URL" in DLS.

3.3 What to do when it does not work in DLS?

– If no dialog comes up, or if the Dialog is empty, when the browse button is pressed

  - Check that the Server is running.
  - Test if DLS can access the server from the configuration page

– File extension is not recognized.

  - Check that the file is accessible from a browser

– Software Deployment Job failed

  - Check that the phone software supports HTTPS

3.4 Can another HTTPS Server be used?

Technically, yes. You can use any HTTPS Server, as long as you use the ASP or PHP script. Therefore, you need to make sure that your server is correctly configured, and supports either ASP 2.0 or PHP. It is, however, not guaranteed that DLS or the OpenStage device works with this HTTP Server, because it was not tested. Extensive testing using a FreeNAS WebService has also been successful in cooperation to DLS. Script presence is still required in this configuration. See point 5 in Ch 3.5 below.

3.5 HTTPS Servers and scanning requirements

Find below some restrictions when deploying phone firmware and media files using an HTTPS server via DLS:

- Deployment via the HTTPS method is <u>only</u> supported by DLS for **OpenStage** phone firmwares and OpenStage-related media files (screensavers, ringertones, logos). The scanner will ignore the presence of `.app` files for optiPoints. This is by design and customers should use the FTP method if required to deploy optiPoint firmwares.

- Ringertones must not exceed 1Mb in size while screensavers/logos should not be larger than 300kb. If not, the files will not be visible in the scanner thus available for deployment. The functionality of the HTTPS server and the DLS scanner itself will not be affected though by the presence of the files. For more details on file deployment restrictions and possible limitations by the devices, please consult the corresponding documentation.

- MIME types should be configured accordingly from within the HTTPS server to allow all necessary possibilities.

- File `file_map.xml` inside `C:\<installation path>\DeploymentService\Tomcat5\webapps\DeploymentService\WEB-INF\classes\` describes the file coverage level from within DLS. As an example, `.gif` files are not supported for screensavers/logos.

- The HTTPS server should allow *Directory Listing* in order to be able to scan subfolder contents. Additionally, copy `dls_directory_reader.asp` or `dls_directory_reader.php` file (depending on the HTTPS server implementation followed), from within the installer DLS folder `\Tools` into the root directory of the HTTPS server.
  In order to check whether or not directory listing is enabled, DLS checks for some strings in the response of the server which are not standardized. So this only works for *Apache Tomcat*, *Apache Webserver (XAMPP)* and *IIS*. Other solution like for example the use of a *FreeNAS* implementation may use other strings to indicate directory listing hence there might be still a need to use the php/asp scripts even if directory listing is enabled from within FreeNAS.

- Please also follow our file/folder naming scheme requirements as much as possible - mentioned in the Release Notes of DLS - in order to avoid failed scans. As an example, special characters should be avoided inside file names.

- Since DLSV3R0 CV744 onwards, files/directories with spaces are now allowed and recognised. Scanned result entries will be fetched with spaces being replaced by the "`%20`" symbol.

- For configuring trusted certificates, please refer to the corresponding documentation for additional information.

3.6 Permission Problems in root path of IIS

DLS recursivly scans through all directories below the path configured as “HTTPS Server URL” in DLS. Since DLS stops the scan in case of errors, any directory which does not allow anonymous access will stop the query of DLS resulting in no or not all firmware images / other device files found from DLS. To avoid this problem it is highly recommended to define a dedicated subdirectory in IIS to store device specific files and provide a URL including this path as “HTTPS Server URL” in Screen “HTTPS Server Configuration” to DLS, e.g. https://downloadserver.com/dls instead https://downloadserver.com.

4 HTTPS for a Linux based environment

The following sections outline a procedure to deploy an HTTPS server for DLS software deployment in a Linux-based server. The benefits of using such an approach is that the customer can rely on an open-source based solution to provide the same functionality and services as by using a proprietary IIS server.

4.1 Prerequisites/Requirements

The basic prerequisite for deploying an Apache-based HTTPS server is any physical or virtual machine that hosts one of the following OSes:

- OpenSuSE 11.4 (or higher)

OR

- SLES 11 SP1 (or higher)

In case, such a server does not exist, the SLES 11 SP1 setup DVD that is used to deploy UC servers can be utilized. However a procedure that outlines the deployment of a SuSE/SLES-based server is beyond the scope of this document.

Depending on whether an OpenSuSE or SLES Linux-based operating system is been deployed, the end-user should obtain the corresponding setup medium (for example a DVD or ISO image or a software repository reachable within the customer’s network infrastructure).
The candidate server that will be used to deploy the Apache HTTPS server should be reachable within the same network as the DLS server and should normally have an FQDN name configured.

Respectively the configured FQDN name should be resolvable using a DNS server.

All actions described in this document need to be held as user **root**.

Even though a thorough knowledge of administering a Linux-based environment is not required, the end-user should at least be able to logon/logoff via a console and be able to use a command-line based text editor like**vi** or **nano.**

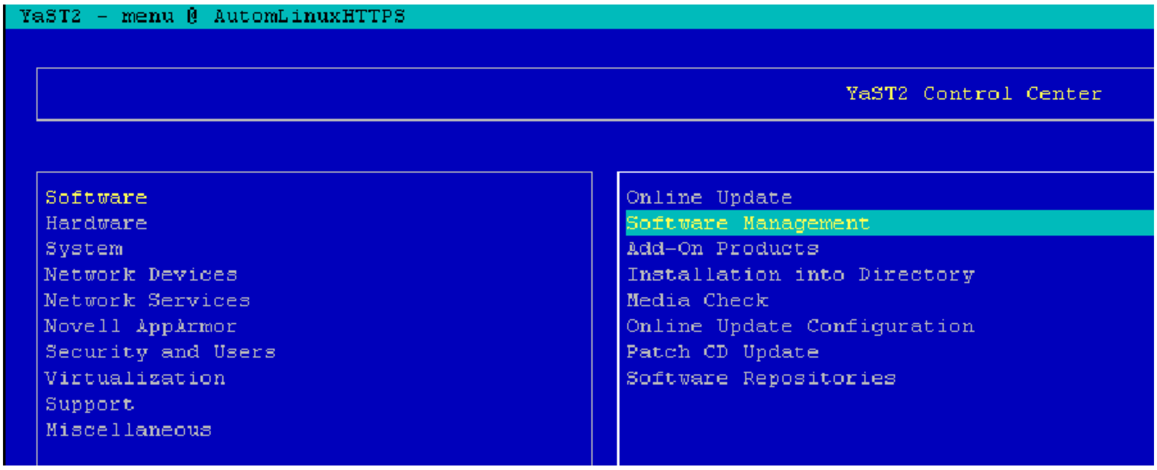
4.2 Installation of Apache packages

Prior of configuring an Apache Server, the end-user must install its corresponding software package(s), either by using the setup DVD medium or a SuSE/SLES software repository.

1. Open a console, login as root to the server and

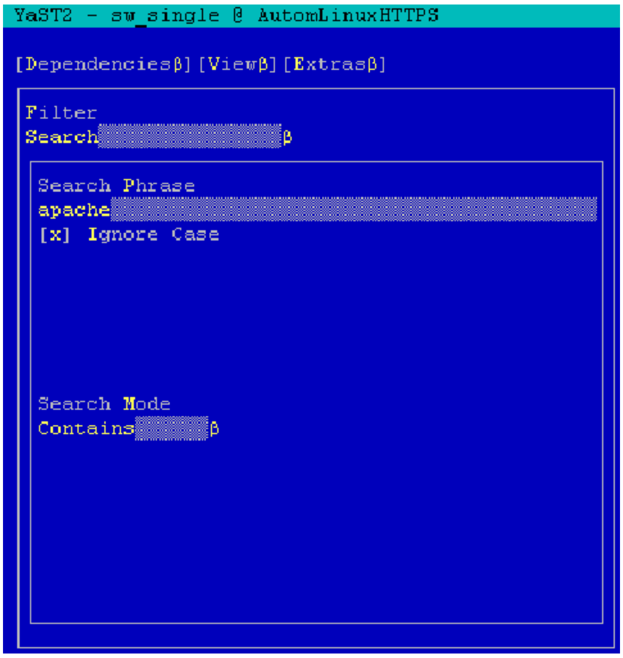
   execute: `4.3 yast`

2. By using the TAB and arrow keys, navigate and select: Software → Software Management



YaST2 - menu @ AutomLinuxHTTPS

3. Go to the “Search Phrase” text field, type the keyword “apache” (without the quotes) and hit <ENTER>.



YaST2 - sw_single @ AutomLinuxHTTPS

Filter
Search

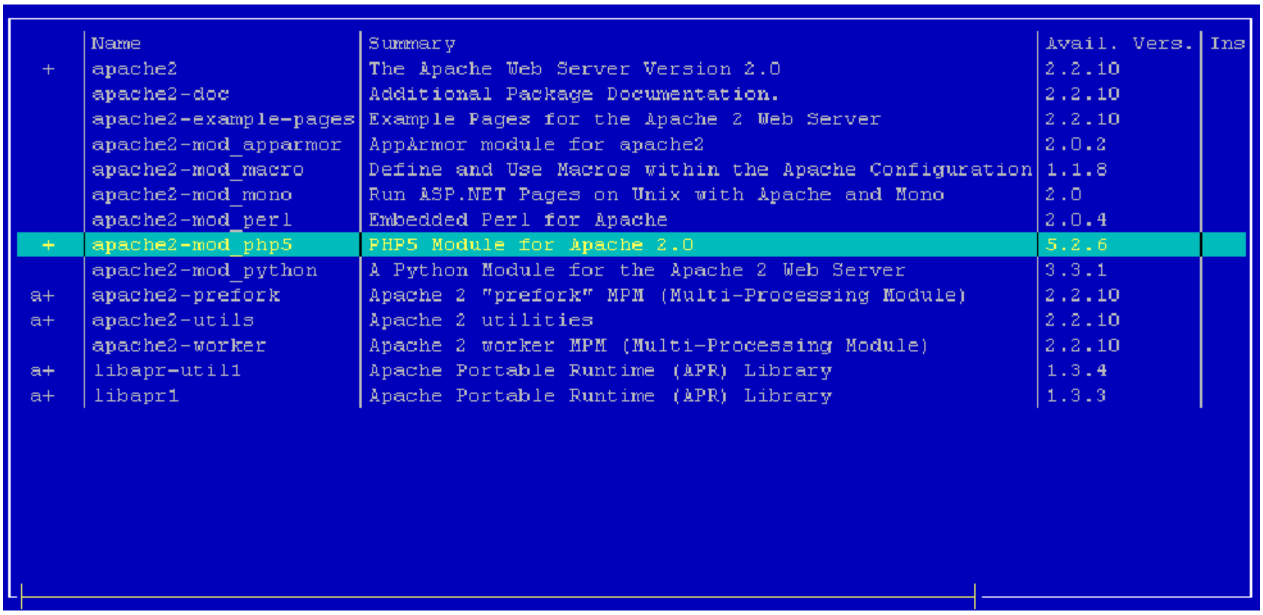
Search Phrase
apache
[x] Ignore Case

Search Mode
Contains

4. On the right side of the screen, the end-user will be presented with all available packages found using the “apache” keyword. By utilizing the TAB and arrow keys, navigate and select the “apache2” package and hit <ENTER>.

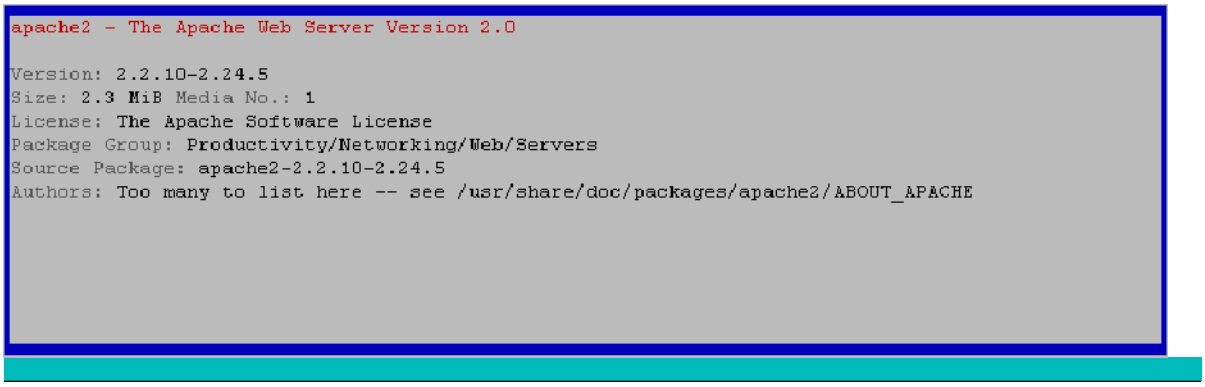
Select the “ **apache2**” and the “ **apache2-mod_php5**” packages.

The YaST tool will automatically resolve if any additional packages are required.



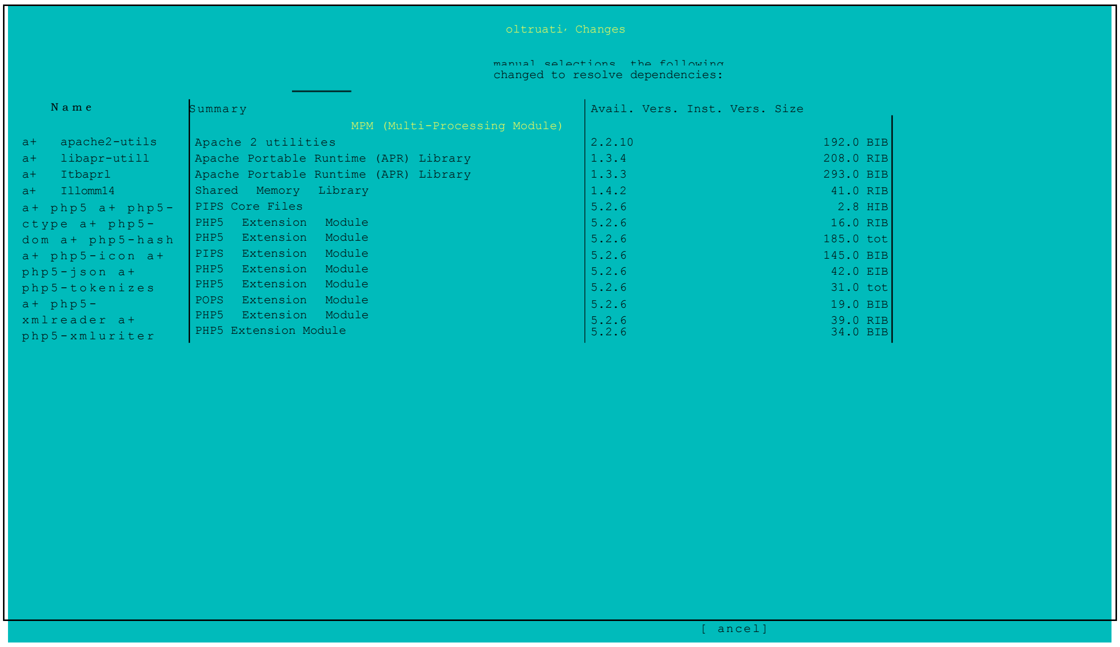
```
     Name                  Summary                                                Avail. Vers. Ins
 +   apache2               The Apache Web Server Version 2.0                      2.2.10
     apache2-doc           Additional Package Documentation.                      2.2.10
     apache2-example-pages Example Pages for the Apache 2 Web Server              2.2.10
     apache2-mod_apparmor  AppArmor module for apache2                            2.0.2
     apache2-mod_macro     Define and Use Macros within the Apache Configuration  1.1.8
     apache2-mod_mono      Run ASP.NET Pages on Unix with Apache and Mono         2.0
     apache2-mod_perl      Embedded Perl for Apache                               2.0.4
 +   apache2-mod_php5      PHP5 Module for Apache 2.0                             5.2.6
     apache2-mod_python    A Python Module for the Apache 2 Web Server            3.3.1
a+   apache2-prefork       Apache 2 "prefork" MPM (Multi-Processing Module)       2.2.10
a+   apache2-utils         Apache 2 utilities                                     2.2.10
     apache2-worker        Apache 2 worker MPM (Multi-Processing Module)          2.2.10
a+   libapr-util1          Apache Portable Runtime (APR) Library                  1.3.4
a+   libapr1               Apache Portable Runtime (APR) Library                  1.3.3
```

5. By using the TAB and arrow keys, navigate and select the “Accept” button and then hit <ENTER>.

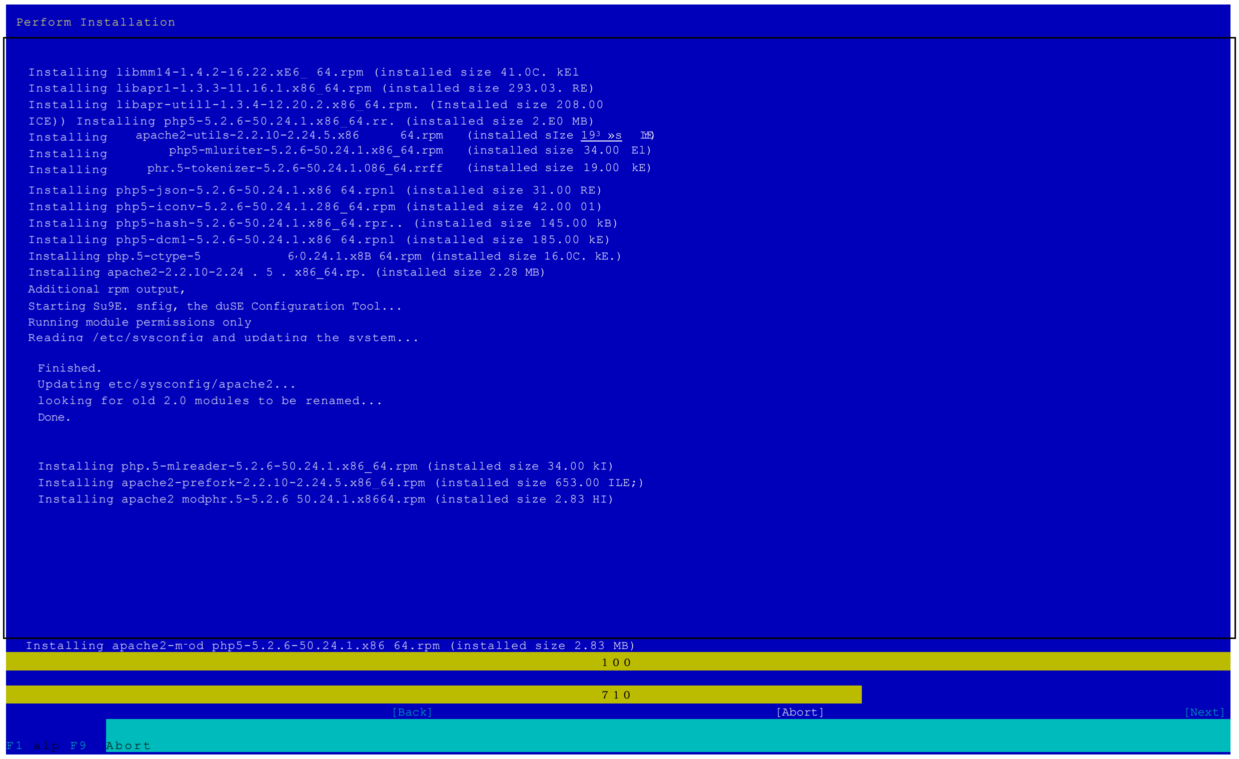


```
apache2 - The Apache Web Server Version 2.0

Version: 2.2.10-2.24.5
Size: 2.3 MiB Media No.: 1
License: The Apache Software License
Package Group: Productivity/Networking/Web/Servers
Source Package: apache2-2.2.10-2.24.5
Authors: Too many to list here -- see /usr/share/doc/packages/apache2/ABOUT_APACHE
```

6. Hit “OK” to proceed



```
                              oltruati‹ Changes

                              manual selections  the following
                              changed to resolve dependencies:

   Name             Summary                                Avail. Vers. Inst. Vers. Size
                               MPM (Multi-Processing Module)
a+  apache2-utils   Apache 2 utilities                     2.2.10                    192.0 BIB
a+  libapr-utill    Apache Portable Runtime (APR) Library  1.3.4                     208.0 RIB
a+  Itbaprl         Apache Portable Runtime (APR) Library  1.3.3                     293.0 BIB
a+  Illomm14        Shared  Memory  Library                1.4.2                      41.0 RIB
a+ php5 a+ php5-    PIPS Core Files                        5.2.6                       2.8 HIB
ctype a+ php5-      PHP5  Extension  Module                5.2.6                      16.0 RIB
dom a+ php5-hash    PHP5  Extension  Module                5.2.6                     185.0 tot
a+ php5-icon a+     PIPS  Extension  Module                5.2.6                     145.0 BIB
php5-json a+        PHP5  Extension  Module                5.2.6                      42.0 EIB
php5-tokenizes      PHP5  Extension  Module                5.2.6                      31.0 tot
a+ php5-            POPS  Extension  Module                5.2.6                      19.0 BIB
xmlreader a+        PHP5  Extension  Module                5.2.6                      39.0 RIB
php5-xmluriter      PHP5 Extension Module                  5.2.6                      34.0 BIB

                                                                 [ ancel]
```

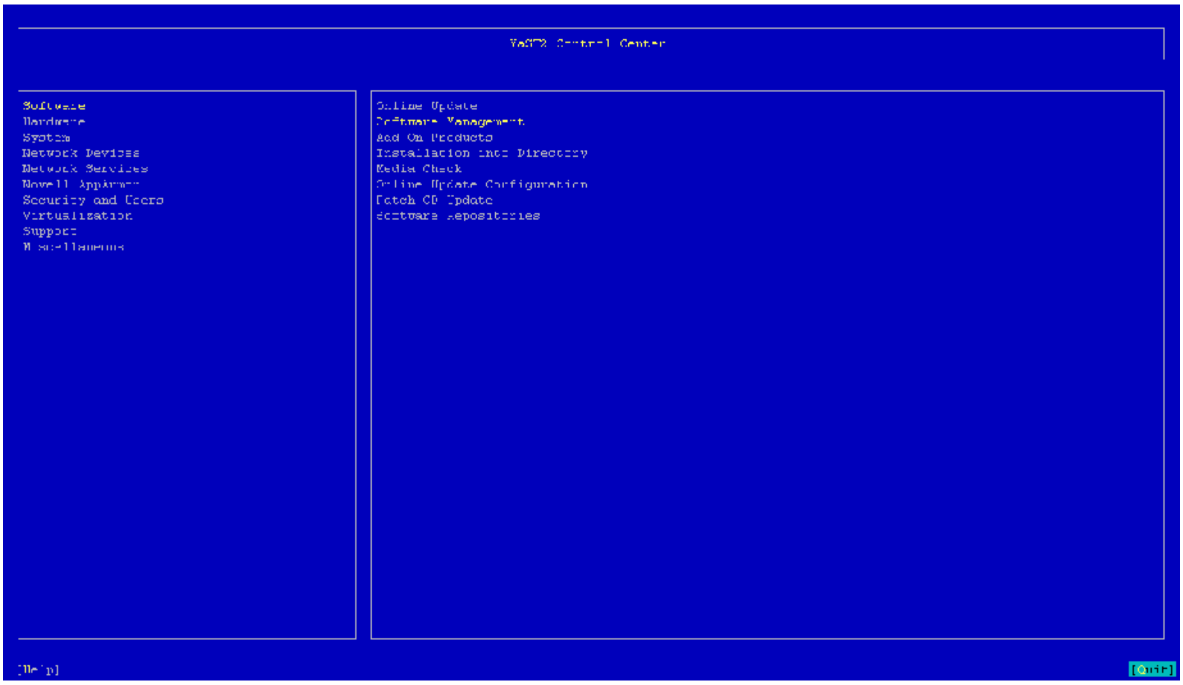


```
Perform Installation

 Installing libmm14-1.4.2-16.22.xE6_ 64.rpm (installed size 41.0C. kEl
 Installing libapr1-1.3.3-11.16.1.x86_64.rpm (installed size 293.03. RE)
 Installing libapr-utill-1.3.4-12.20.2.x86_64.rpm. (Installed size 208.00
 ICE)) Installing php5-5.2.6-50.24.1.x86_64.rr. (installed size 2.E0 MB)
 Installing    apache2-utils-2.2.10-2.24.5.x86     64.rpm   (installed sIze 19³ »s   IE)
 Installing         php5-mluriter-5.2.6-50.24.1.x86_64.rpm   (installed size 34.00  El)
 Installing     phr.5-tokenizer-5.2.6-50.24.1.086_64.rrff   (installed size 19.00  kE)
 Installing php5-json-5.2.6-50.24.1.x86 64.rpnl (installed size 31.00 RE)
 Installing php5-iconv-5.2.6-50.24.1.286_64.rpm (installed size 42.00 01)
 Installing php5-hash-5.2.6-50.24.1.x86_64.rpr.. (installed size 145.00 kB)
 Installing php5-dcml-5.2.6-50.24.1.x86 64.rpnl (installed size 185.00 kE)
 Installing php.5-ctype-5           6‹0.24.1.x8B 64.rpm (installed size 16.0C. kE.)
 Installing apache2-2.2.10-2.24 . 5 . x86_64.rp. (installed size 2.28 MB)
 Additional rpm output,
 Starting Su9E. snfig, the duSE Configuration Tool...
 Running module permissions only
 Reading /etc/sysconfig and updating the system...

  Finished.
  Updating etc/sysconfig/apache2...
  looking for old 2.0 modules to be renamed...
  Done.


  Installing php.5-mlreader-5.2.6-50.24.1.x86_64.rpm (installed size 34.00 kI)
  Installing apache2-prefork-2.2.10-2.24.5.x86_64.rpm (installed size 653.00 ILE;)
  Installing apache2 modphr.5-5.2.6 50.24.1.x8664.rpm (installed size 2.83 HI)

Installing apache2-m-od php5-5.2.6-50.24.1.x86 64.rpm (installed size 2.83 MB)
                                   100

                                   710
                    [Back]                        [Abort]                        [Next]
F1 alp F9  Abort
```

7. **Installation of required packages will initiate**

8. **Exit the YaST tool by using the TAB and Arrow keys and selecting "Quit"**

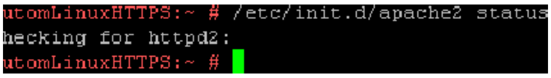
10/2019 Unify Communications



9. Check the status of the “apache2” service. Execute:

```
/etc/init.d/apache2 status
```

Normally it should be in status “unused”.



```
utomLinuxHTTPS:~ # /etc/init.d/apache2 status
hecking for httpd2:
utomLinuxHTTPS:~ #
```

4.3 Firewall Settings

Prior of deploying the HTTPS service, the end-user needs to check if the firewall is up and running and apply changes accordingly. This section outlines the steps required to make such changes.

1. The end-user needs to check if a firewall is up and running. Execute the following commands:

   - Check the operating status of the firewall

   service: `rcSuSEfirewall2 status`

   - If the above command indicates that a firewall is running, then check what is being allowed and configured by issuing the following command:

   ```
   iptables -L
   ```

2. Make sure that access is allowed to the HTTP(s) ports and thus, the server can be reached. The supplied configurations are called `apache2` and `apache2-ssl`. They can be enabled either:

- Via YaST, by adding them to `FW_CONFIGURATIONS_EXT` in `/etc/sysconfig/SuSEfirewall2`

OR

- By issuing the following commands,

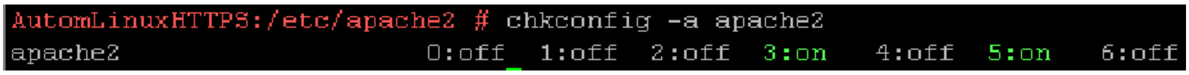
```
sysconf_addword /etc/sysconfig/SuSEfirewall2 FW_CONFIGURATIONS_EXT
apache2
sysconf_addword /etc/sysconfig/SuSEfirewall2 FW_CONFIGURATIONS_EXT
apache2-ssl
rcSuSEfirewall2 restart
```

4.4 Starting the server in HTTP mode

Start the server and configure it to automatically start at boot time (enable its operation at runlevels 3 and 5).

Execute the following commands:

```
rcapache2 start
chkconfig -a apache2
```

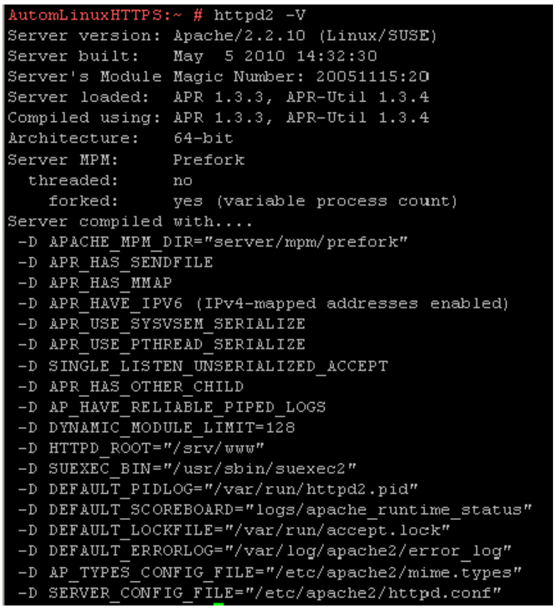


```
AutomLinuxHTTPS:/etc/apache2 # chkconfig -a apache2
apache2                   0:off  1:off  2:off  3:on   4:off  5:on   6:off
```

At this point the apache server should run in HTTP mode. Currently, the default `DocumentRoot` where files can be put, is at `/srv/www/htdocs`

To check what version of Apache is installed and important files/directories are located for this box, execute:

```
httpd2 -V
```



```
AutomLinuxHTTPS:~ # httpd2 -V
Server version: Apache/2.2.10 (Linux/SUSE)
Server built:   May  5 2010 14:32:30
Server's Module Magic Number: 20051115:20
Server loaded:  APR 1.3.3, APR-Util 1.3.4
Compiled using: APR 1.3.3, APR-Util 1.3.4
Architecture:   64-bit
Server MPM:     Prefork
  threaded:     no
    forked:     yes (variable process count)
Server compiled with....
 -D APACHE_MPM_DIR="server/mpm/prefork"
 -D APR_HAS_SENDFILE
 -D APR_HAS_MMAP
 -D APR_HAVE_IPV6 (IPv4-mapped addresses enabled)
 -D APR_USE_SYSVSEM_SERIALIZE
 -D APR_USE_PTHREAD_SERIALIZE
 -D SINGLE_LISTEN_UNSERIALIZED_ACCEPT
 -D APR_HAS_OTHER_CHILD
 -D AP_HAVE_RELIABLE_PIPED_LOGS
 -D DYNAMIC_MODULE_LIMIT=128
 -D HTTPD_ROOT="/srv/www"
 -D SUEXEC_BIN="/usr/sbin/suexec2"
 -D DEFAULT_PIDLOG="/var/run/httpd2.pid"
 -D DEFAULT_SCOREBOARD="logs/apache_runtime_status"
 -D DEFAULT_LOCKFILE="/var/run/accept.lock"
 -D DEFAULT_ERRORLOG="/var/log/apache2/error_log"
 -D AP_TYPES_CONFIG_FILE="/etc/apache2/mime.types"
 -D SERVER_CONFIG_FILE="/etc/apache2/httpd.conf"
```

4.5 Enable SSL and generate self-signed keys

In order for the apache server to operate in HTTPS mode, the end-user needs to make sure that Apache starts with certain modules enabled.

1. `Enable the SSL module.` Execute the following

   command: `a2enmod ssl`

   The “a2enmod” command adapts `APACHE_MODULES` in `/etc/sysconfig/apache2`

   If a message is displayed indicating that the module is already present, ignore it.

2. Check if the “php” module exists (if not, it will be enabled) Execute:

   ```
   a2enmod php5
   ```

   If a message is displayed indicating that the module is already present, ignore it.

3. Insert the “rewrite” module. Execute:

   ```
   a2enmod rewrite
   ```

   If a message is displayed indicating that the module is already present, ignore it.

4. The next step would be enabling the SSL module within Apache with a script called “a2enflag”. Similarly to the command above it changes `APACHE_SERVER_FLAGS`. Execute:

   ```
   a2enflag SSL
   ```

   The “a2enflag” command modifies the “/etc/sysconfig/apache2” file from:

   ```
   APACHE_SERVER_FLAGS=""
   ```

   to

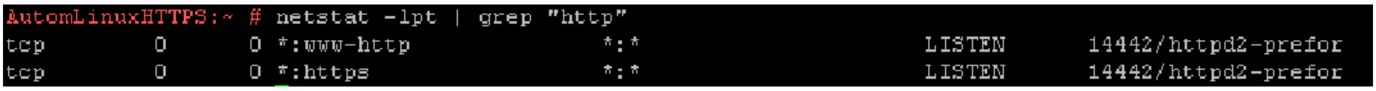
   ```
   APACHE_SERVER_FLAGS="SSL"
   ```

5. Restart Apache. Execute:

   ```
   rcapache2 restart
   ```

6. Check if the machine listens for http and https traffic.

   Execute: `netstat -lpt | grep "http"`



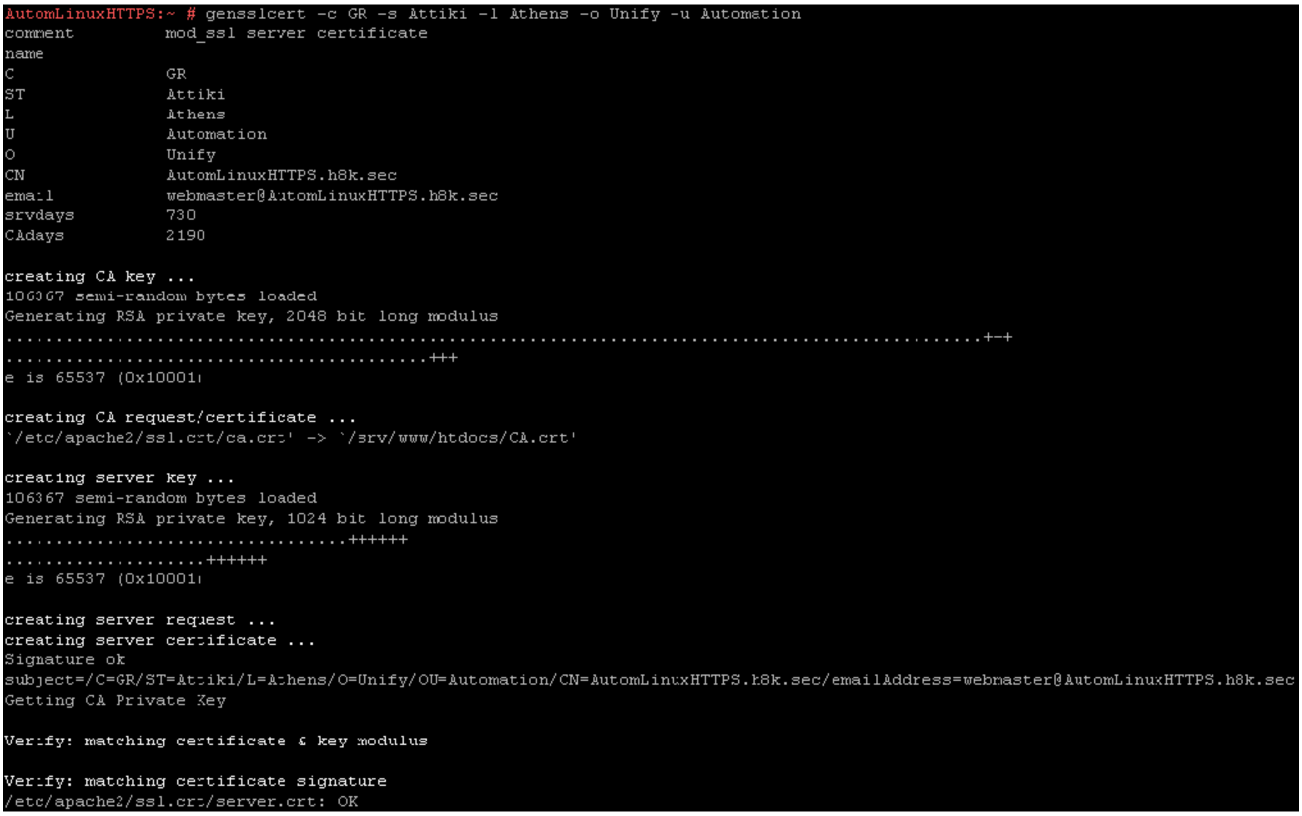
```
AutomLinuxHTTPS:~ # netstat -lpt | grep "http"
tcp        0      0 *:www-http              *:*                     LISTEN      14442/httpd2-prefor
tcp        0      0 *:https                 *:*                     LISTEN      14442/httpd2-prefor
```

7. Generate self-signed keys. Execute the following command, by providing the appropriate information:

```
   gensslcert -c <COUNTRY_PREFIX> -s <STATE/REGION> -l <CITY> -o
<COMPANY> -u <ORGANIZATIONAL_UNIT>
```

Reference Example:

```
gensslcert -c GR -s Attiki -l Athens -o Unify -u Automation
```



```
AutomLinuxHTTPS:~ # gensslcert -c GR -s Attiki -l Athens -o Unify -u Automation
comment          mod_ssl server certificate
name
C                GR
ST               Attiki
L                Athens
U                Automation
O                Unify
CN               AutomLinuxHTTPS.h8k.sec
email            webmaster@AutomLinuxHTTPS.h8k.sec
srvdays          730
CAdays           2190

creating CA key ...
106367 semi-random bytes loaded
Generating RSA private key, 2048 bit long modulus
.......................................................................................................+-+
..........................................+++
e is 65537 (0x10001)

creating CA request/certificate ...
`/etc/apache2/ssl.crt/ca.crt' -> `/srv/www/htdocs/CA.crt'

creating server key ...
106367 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
..................................++++++
...................++++++
e is 65537 (0x10001)

creating server request ...
creating server certificate ...
Signature ok
subject=/C=GR/ST=Attiki/L=Athens/O=Unify/OU=Automation/CN=AutomLinuxHTTPS.h8k.sec/emailAddress=webmaster@AutomLinuxHTTPS.h8k.sec
Getting CA Private Key

Verify: matching certificate & key modulus

Verify: matching certificate signature
/etc/apache2/ssl.crt/server.crt: OK
```

Based on the flags used for the “gensslcert” command, it can be noted that as a “Common Name” (aka CN), the certificate uses automatically the FQDN of the server. If no FQDN has been defined, then as a “Common Name” the server’s IP address is utilized.

The “gensslcert” command (over)writes these files:

```
/etc/apache2/ssl.crt/ca.crt
/etc/apache2/ssl.key/server.key
/etc/apache2/ssl.crt/server.crt
/etc/apache2/ssl.csr/server.csr
```

A copy of `ca.crt` is also created at `/srv/www/htdocs/` and becomes available for download.

4.6 Create a Virtual host

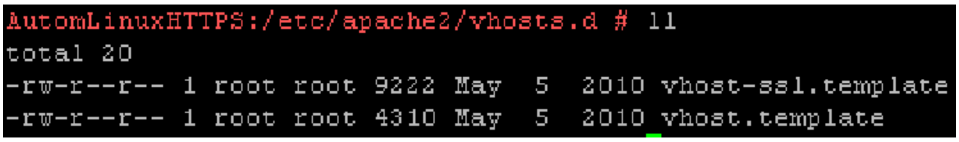
In order for the Apache server to operate in HTTPS mode, a virtual host needs to be created. This section outlines the steps required to accomplish this task.

1. The virtual host configuration files are located at the `/etc/apache2/vhosts.d/` directory.

   Go to that directory:

   ```
   cd /etc/apache2/vhosts.d/
   ```

   As it can be noted, there are two configuration templates, one for use **with ssl** and one **without ssl** .



```
AutomLinuxHTTPS:/etc/apache2/vhosts.d # ll
total 20
-rw-r--r-- 1 root root 9222 May  5  2010 vhost-ssl.template
-rw-r--r-- 1 root root 4310 May  5  2010 vhost.template
```

   The template **with ssl** will be used.

2. Define a virtual host

   There are two ways to define a virtual host:

   - Using a configured FQDN (method 1)
   - Using the server's IP address (method 2)

   METHOD 1:

   If an FQDN has been configured for this server , then make a copy of the sample configuration file `vhost-ssl.template` to `<hostname>.conf` and create the corresponding to-be-utilized directory

   Execute:

   ```
   cp vhost-ssl.template <hostname>.conf
   mkdir -p /srv/www/vhosts/<hostname>/
   ```

   Reference example:

   ```
   cp vhost-ssl.template AutomLinuxHTTPS.conf
   mkdir -p /srv/www/vhosts/AutomLinuxHTTPS/
   ```

METHOD 2:

If no FQDN has been configured OR the end-user does not want to use an FQDN, then as a simpler approach make a copy of the sample configuration file `vhost-ssl.template` to `<ipaddress>.conf` and create the corresponding to-be-utilized directory.

To find the IP address, execute:

```
ifconfig | grep "inet addr" | awk -F: '{print $2}' | awk '{print $1}'
| grep -v '127.0.0.1'

OR

ifconfig | grep -Eo 'inet (addr:)?([0-9]*\.){3}[0-9]*' | grep -Eo
'([0-9]*\.){3}[0-9]*' | grep -v '127.0.0.1'
```

Make the copy and create the corresponding directory, execute:

```
cp vhost-ssl.template <ipaddress>.conf
mkdir -p /srv/www/vhosts/<ipaddress>/
```

Reference example:

```
mkdir -p /srv/www/vhosts/10.10.72.33/
```

3. Whether "<`hostname>.conf`" or "`<ipaddress>.conf` configuration file has been created in the previous step, it needs to be edited as outlined below.

If METHOD 1 has been used (hostname) from the previous step , then

a. Open the `<hostname>.conf` file using a text editor (located at the `/etc/apache2/vhosts.d/` directory).

b. Find the following line:

```
DocumentRoot "/srv/www/htdocs"
```

And change it to:

```
DocumentRoot "/srv/www/vhosts/<hostname>"
```

Reference Example:

```
DocumentRoot "/srv/www/vhosts/AutomLinuxHTTPS"
```

c. Then, find the following XML element:

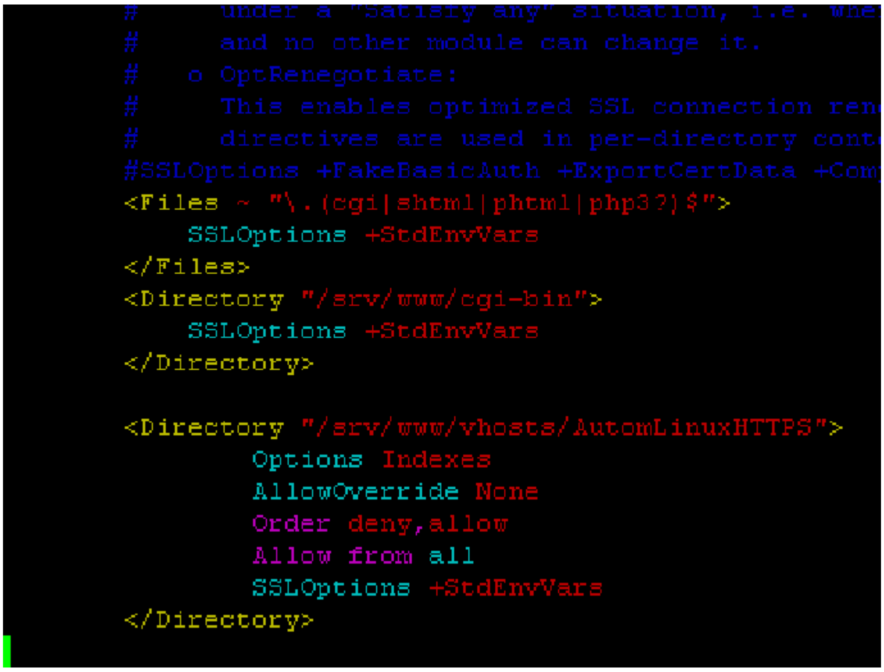
```
<Directory "/srv/www/cgi-bin">
   SSLOptions +StdEnvVars
   </Directory>
```

Below the "`</Directory>`" closing tag, add the following XML Element:

```
<Directory "/srv/www/vhosts/<hostname>">
      Options Indexes
      AllowOverride None
      Order deny,allow
      Allow from all
      SSLOptions +StdEnvVars
</Directory>
```

Reference Example:

```
<Directory "/srv/www/vhosts/AutomLinuxHTTPS">
      Options Indexes
      AllowOverride None
      Order deny,allow
      Allow from all
      SSLOptions +StdEnvVars
</Directory>
```



```
#     under a "Satisfy any" situation, i.e. whe
#     and no other module can change it.
#   o OptRenegotiate:
#     This enables optimized SSL connection ren
#     directives are used in per-directory cont
#SSLOptions +FakeBasicAuth +ExportCertData +Com
<Files ~ "\.(cgi|shtml|phtml|php3?)$">
    SSLOptions +StdEnvVars
</Files>
<Directory "/srv/www/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>

<Directory "/srv/www/vhosts/AutomLinuxHTTPS">
        Options Indexes
        AllowOverride None
        Order deny,allow
        Allow from all
        SSLOptions +StdEnvVars
</Directory>
```

If METHOD 2 (IP address) has been used from the previous step , then

a. Open the `<ipaddress>.conf` file using a text editor (located at the `/etc/apache2/vhosts.d/` directory)

b. Find the following line:

```
DocumentRoot "/srv/www/htdocs"
```

And change it to:

```
DocumentRoot "/srv/www/vhosts/<ipaddress>"
```

Reference Example:

```
DocumentRoot "/srv/www/vhosts/10.10.72.33"
```

c. Find the following XML element:

```
<Directory "/srv/www/cgi-bin">
   SSLOptions +StdEnvVars
   </Directory>
```

Below the "`</Directory>`" closing tag, add the following XML Element:

```
<Directory "/srv/www/vhosts/<ipaddress>">
      Options Indexes
      AllowOverride None
      Order deny,allow
      Allow from all
      SSLOptions +StdEnvVars
</Directory>
```

Reference Example:

```
<Directory "/srv/www/vhosts/10.10.72.33">
      Options Indexes
      AllowOverride None
      Order deny,allow
      Allow from all
      SSLOptions +StdEnvVars
</Directory>
```

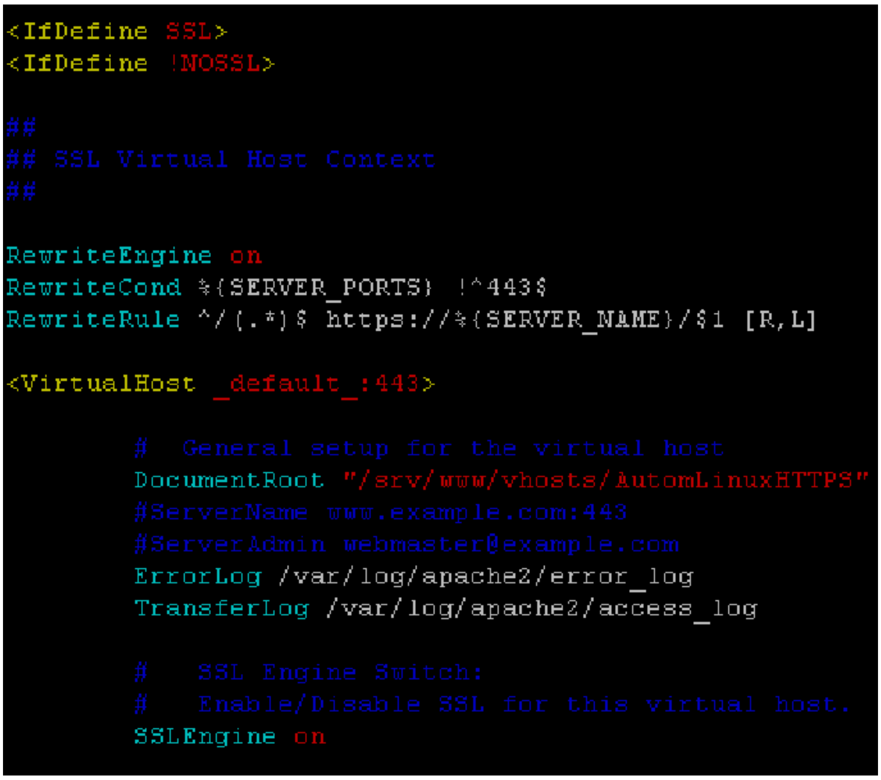
4. As a final modification step, the end-user needs to add the following lines at the "`<hostname>.conf`" or "`<ipaddress>.conf`" file (depending on which of the two methods has been used). This change will ensure that HTTP will be automatically re-directed to HTTPS:

   Find the following 2 lines:

```
<IfDefine SSL>
<IfDefine !NOSSL>
```

And just below them, add the following ones:

```
RewriteEngine on
RewriteCond %{SERVER_PORTS} !^443$
RewriteRule ^/(.*)$ https://%{SERVER_NAME}/$1 [R,L]
```



```
<IfDefine SSL>
<IfDefine !NOSSL>

##
## SSL Virtual Host Context
##

RewriteEngine on
RewriteCond %{SERVER_PORTS} !^443$
RewriteRule ^/(.*)$ https://%{SERVER_NAME}/$1 [R,L]

<VirtualHost _default_:443>

        #  General setup for the virtual host
        DocumentRoot "/srv/www/vhosts/AutomLinuxHTTPS"
        #ServerName www.example.com:443
        #ServerAdmin webmaster@example.com
        ErrorLog /var/log/apache2/error_log
        TransferLog /var/log/apache2/access_log

        #   SSL Engine Switch:
        #   Enable/Disable SSL for this virtual host.
        SSLEngine on
```

5. If method 1 is used (hostname) for the creation of the virtual host configuration file, then by using software like WinSCP or Filezilla, phones' firmware should be placed at the following directory (as created at step 2):

```
/srv/www/vhosts/<hostname>
```

Reference Example:

```
/srv/www/vhosts/AutomLinuxHTTPS
```

If method 2 is used (IP address) for the creation of the virtual host configuration file, phones' firmware should be placed at the following directory (as created at step 2):

```
/srv/www/vhosts/<ipaddress>
```

Reference Example:

```
/srv/www/vhosts/10.10.72.33
```

6. The apache service needs to be restarted in order for the changes to be digested. Execute:

```
/etc/init.d/apache2 restart
```

4.7 Providing an additional Listening port

In case an additional listening port needs to be configured (which will be automatically redirected to the default secure one (443), the following steps outline how to accomplish such a task. In this case, port 444 is utilized. However, the end-user can define any desired port number as long as it is not reserved.

1. Go to the following directory:

```
cd /etc/apache2
```

2. Using an editor, open the file “listen.conf”

3. Find the following line:

And just below it, add the following:

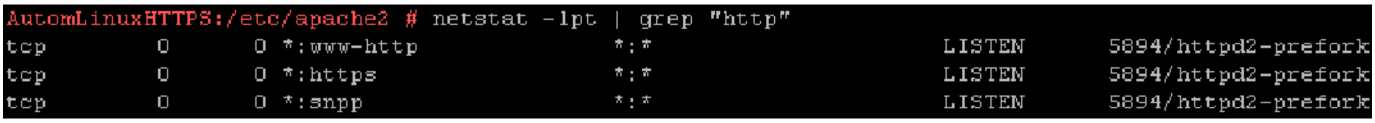
```
Listen 444
```

4. Close the editor. In for the Apache server to digest the changes, it needs to be restarted. Execute:

```
/etc/init.d/apache2 restart
```

5. Check that the Apache server now listens to an additional port.

   Execute: `netstat -lpt | grep "http"`



```
AutomLinuxHTTPS:/etc/apache2 # netstat -lpt | grep "http"
tcp        0      0 *:www-http              *:*                     LISTEN      5894/httpd2-prefork
tcp        0      0 *:https                 *:*                     LISTEN      5894/httpd2-prefork
tcp        0      0 *:snpp                  *:*                     LISTEN      5894/httpd2-prefork
```

4.8 Troubleshooting

Any generated error messages can be read when the “apache2” service has started. Reproduce what is not working and see how it is reflected in the logs. The log files can be monitored in a root shell by issuing the following command:

```
tail -F /var/log/apache2/*
```

To check the SSL Virtual Host setup, execute:

```
httpd2 -S –DSSL
```

To check which shared modules are present, execute:

```
httpd2 -M
```

5 REFERENCES

[1] xampp, http://www.apachefriends.org/en/xampp.html

[2] IIS Resource, http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/993a8a36-5761-448f-889e-9ae58d072c09.mspx?mfr=true

[3] How to create self-signed SSL Certificate, http://www.somacon.com/p42.php

[4] Apache HTTP Server Installation, http://httpd.apache.org/docs/2.2/install.html

[5] Apache HTTP Server Security Tips, http://httpd.apache.org/docs/2.2/misc/security_tips.html

[6] XAMPP Security, http://www.apachefriends.org/en/xampp-windows.html#1221

[7] Installing and Securing IIS Servers (Part 1), http://www.windowsecurity.com/articles/Installing_Securing_IIS_Servers_Part1.html

[8] ASP.NET installation for IIS 6.0, http://www.asp.net/learn/whitepapers/aspnet-and-iis6/

[9] .Net Framework 2.0, http://www.microsoft.com/downloads/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5&displaylang=en

Bibliography

e.g. /1/	e.g. M1-Binder, V1, 2005-03-11, Miller, Com ESY HD..

Table 1 Bibliography

Abbreviations / Definitions / Glossary / Terminology

Abbreviation	Definition
AMO	Administration and Maintenance Order (HiPath 4000)
BLS	Back Level Support
DHCP	Dynamic Host Configuration Protocol
DLS	Deployment Service
DNS	Domain Name System
FDB	Feature Documentation Building Block
FTP	File Transfer Protocol
GVS	Global Vendor Support
GUI	Graphical User Interface
HiSPA	HiPath Serviceability Platform for Applications
HOT	HiPath One Tool, service tool to service the HiPath 4000 system
HTS	HiPath Tele Service
HUGT	HiPath Universal Generation Tool, service tool to generate the HiPath database
HW	Hardware
ID	Request-Number, e-g- RQ00012345
MAC	Moves, Adds and Changes
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NetInfo	Configuration Management for FDBs
NLS	National Language Support
OEM	Original Equipment Manufacturer
Prisma	System to archive SW
RAS	Reliability, Availability, Serviceability
RAS	Remote Access Service
SIRA	Secure Infrastructure for Remote Access
SMP	System Maintenance Package
SMR	System Maintenance Release
SW	Software
SWS	Software Supply Server
TAP	Techniker Arbeitsplatz, notebook used by the service technician
TopInfo-R	Configuration Management for change requests
UI	User Interface

Table 2 Abbreviations / Definitions / Glossary / Terminology

mitel.com