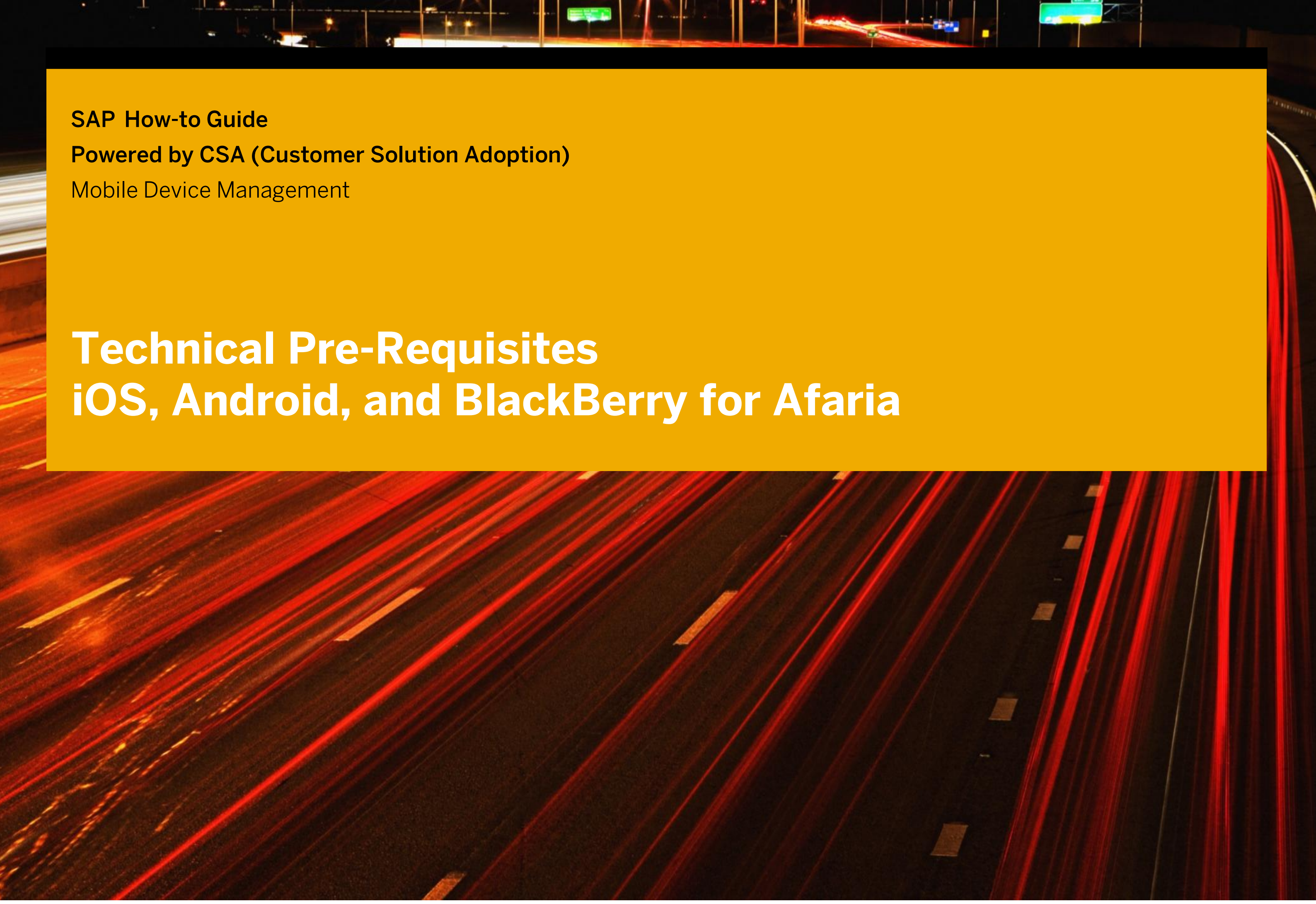


SAP How-to Guide
Powered by CSA (Customer Solution Adoption)
Mobile Device Management

Technical Pre-Requisites iOS, Android, and BlackBerry for Afaria

Applicable Releases:

Afaria 6.6 FP1 Hot Fix 06

Version 1.0

January 2012

The Best-Run Businesses Run SAP™

SAP “How-to” Guides are intended to simplify the product implementation. While specific product features and procedures typically are explained in a practical business context, it is not implied that those features and procedures are the only approach in solving a specific business problem using SAP NetWeaver. Should you wish to receive additional information, clarification or support, please refer to SAP Consulting.

Any software coding and/or code lines / strings (“Code”) included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressively prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP’s Support Services and may not be modified or altered in any way.

The Best-Run Businesses Run SAP™

Document History

Document Version	Description
1.0	Initial release of the document, 01/26/2012

Note

Please forward any comments on this document to: shival.tailor@sap.com

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
`Example text`	File and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	User entry texts. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, `F2` or `ENTER`.

Icons

Icon	Description
⚠	Caution
💡	Note or Important
❖	Example
⬆	Recommendation or Tip

The Best-Run Businesses Run SAP™

Table of Contents

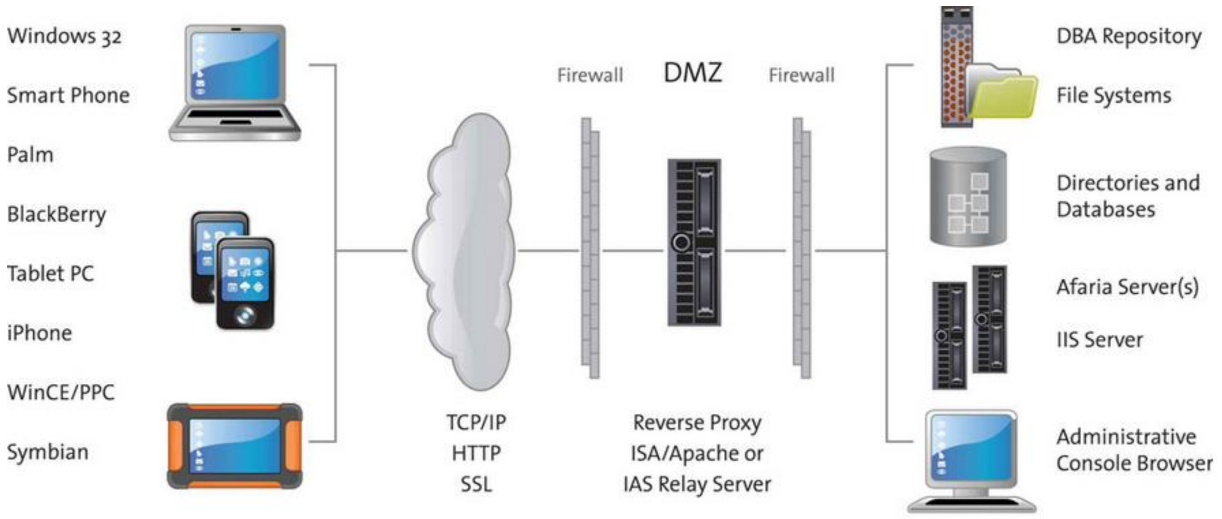
1. Business Scenario

This document gives an overview on the technical pre-requisites for Afaria implementations for Mobile Device Management landscapes. These pre-requisites are advised to be checked prior to the installation.

2. Background Information

This document focuses on a single server environment only with Relay Server included in DMZ. In a single server environment all Afaria components are installed on a same server. Relay Server is an optional component but is highly recommended because of the security aspects. Relay Server typically gets installed in a DMZ environment.

Following is a sample diagram of Afaria architecture:



For iOS landscapes, Enterprise Developer's Registration with Apple is mandatory which may take up to two weeks. There is an alternative procedure for a POC like setups. APNS certificate can be issued by submitting a request to Sybase. This procedure is also covered in this document.

For Android landscapes, C2DM registration is mandatory. The procedure is included in this document.

3. Step-by-Step Pre-requisites

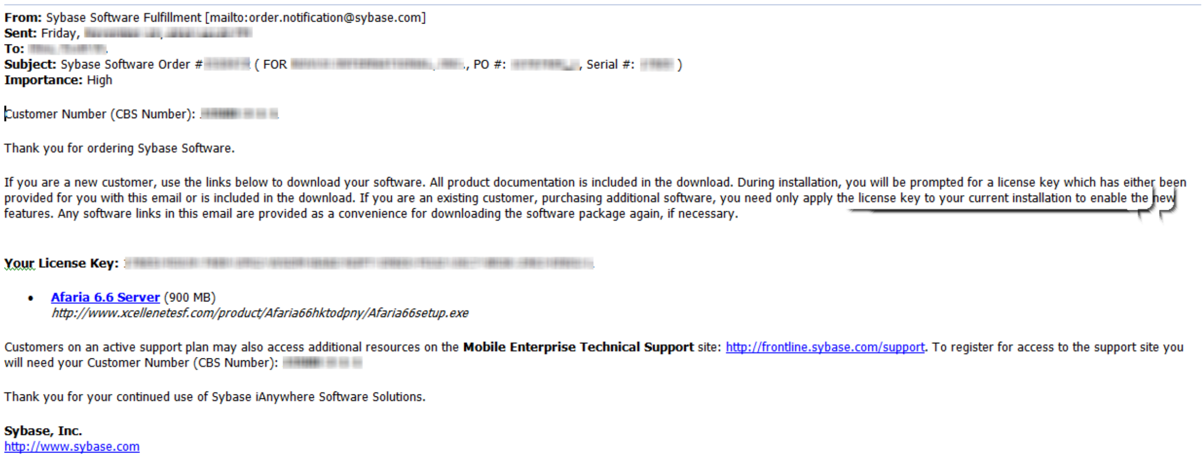
Assuming that the reader of this document has a technical know-how for basic Computer Networking.

3.1 License and Media Download

Afaria license should already be available to initialize the installation. The software media link is usually included in the license key email and should be readily available. Customer may obtain a trial license from Sybase.

Additionally, Afaria software media should be downloaded by Customer, to be placed locally on the Afaria server and accessible from the Relay Server.

A typical email with License key would look like following (sent by Sybase Software Fulfillment [mailto:order.notification@sybase.com]):



From: Sybase Software Fulfillment [mailto:order.notification@sybase.com]
Sent: Friday, [redacted]
To: [redacted].
Subject: Sybase Software Order #[redacted] (FOR [redacted]., PO #: [redacted], Serial #: [redacted])
Importance: High

Customer Number (CBS Number): [redacted]

Thank you for ordering Sybase Software.

If you are a new customer, use the links below to download your software. All product documentation is included in the download. During installation, you will be prompted for a license key which has either been provided for you with this email or is included in the download. If you are an existing customer, purchasing additional software, you need only apply the license key to your current installation to enable the new features. Any software links in this email are provided as a convenience for downloading the software package again, if necessary.

Your License Key: [redacted]

- **Afaria 6.6 Server** (900 MB)
  http://www.xcellenetesf.com/product/Afaria66hktodpny/Afaria66setup.exe

Customers on an active support plan may also access additional resources on the **Mobile Enterprise Technical Support** site: http://frontline.sybase.com/support. To register for access to the support site you will need your Customer Number (CBS Number): [redacted]

Thank you for your continued use of Sybase iAnywhere Software Solutions.

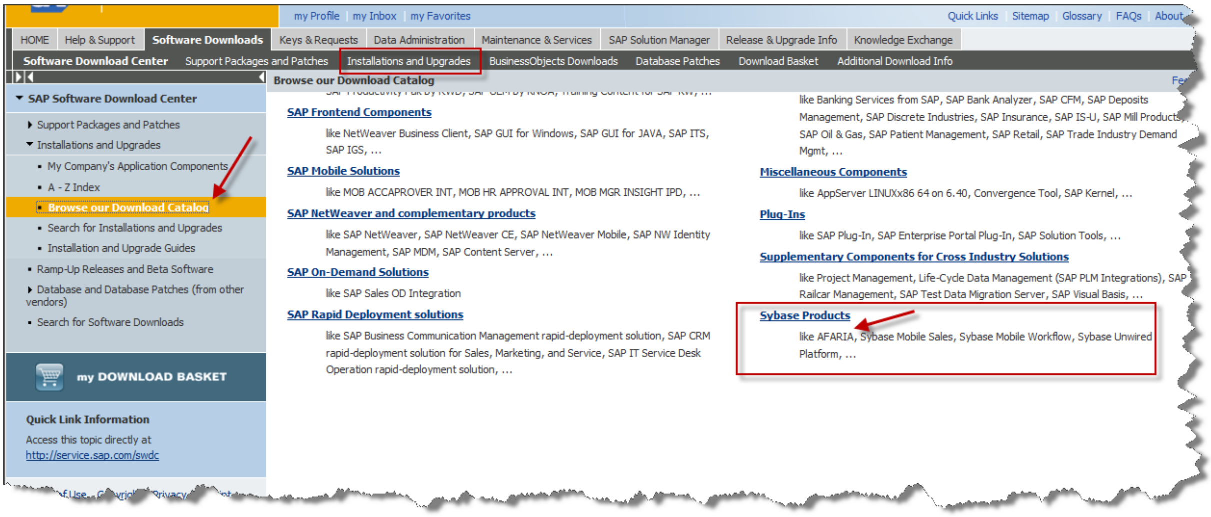
Sybase, Inc.
http://www.sybase.com

A sample of the download link is as following.

http://www.xcellenetesf.com/product/Afaria66hktodpny/Afaria66setup.exe

The can be downloaded from either of the two methods below:

1. By signing-up and logging on to http://frontline.sybase.com web-site or
2. By logging on to SAP Service Marketplace from the software download area, https://service.sap.com/swdc
   The screenshots to download Afaria from SAP Service Marketplace are as following:


my Profile | my Inbox | my Favorites
Quick Links | Sitemap | Glossary | FAQs | About
HOME
Help & Support
Software Downloads
Keys & Requests
Data Administration
Maintenance & Services
SAP Solution Manager
Release & Upgrade Info
Knowledge Exchange
Software Download Center
Support Packages and Patches
Installations and Upgrades
BusinessObjects Downloads
Database Patches
Download Basket
Additional Download Info
SAP Software Download Center
Support Packages and Patches
Installations and Upgrades
My Company's Application Components
A - Z Index
Browse our Download Catalog
Search for Installations and Upgrades
Installation and Upgrade Guides
Ramp-Up Releases and Beta Software
Database and Database Patches (from other vendors)
Search for Software Downloads
my DOWNLOAD BASKET

Quick Link Information

Access this topic directly at http://service.sap.com/swdc

Browse our Download Catalog

SAP Frontend Components

like NetWeaver Business Client, SAP GUI for Windows, SAP GUI for JAVA, SAP ITS, SAP IGS, ...

SAP Mobile Solutions

like MOB ACCAPROVER INT, MOB HR APPROVAL INT, MOB MGR INSIGHT IPD, ...

SAP NetWeaver and complementary products

like SAP NetWeaver, SAP NetWeaver CE, SAP NetWeaver Mobile, SAP NW Identity Management, SAP MDM, SAP Content Server, ...

SAP On-Demand Solutions

like SAP Sales OD Integration

SAP Rapid Deployment solutions

like SAP Business Communication Management rapid-deployment solution, SAP CRM rapid-deployment solution for Sales, Marketing, and Service, SAP IT Service Desk Operation rapid-deployment solution, ...

like Banking Services from SAP, SAP Bank Analyzer, SAP CFM, SAP Deposits Management, SAP Discrete Industries, SAP Insurance, SAP IS-U, SAP Mill Products, SAP Oil & Gas, SAP Patient Management, SAP Retail, SAP Trade Industry Demand Mgmt, ...

Miscellaneous Components

like AppServer LINUXx86 64 on 6.40, Convergence Tool, SAP Kernel, ...

Plug-Ins

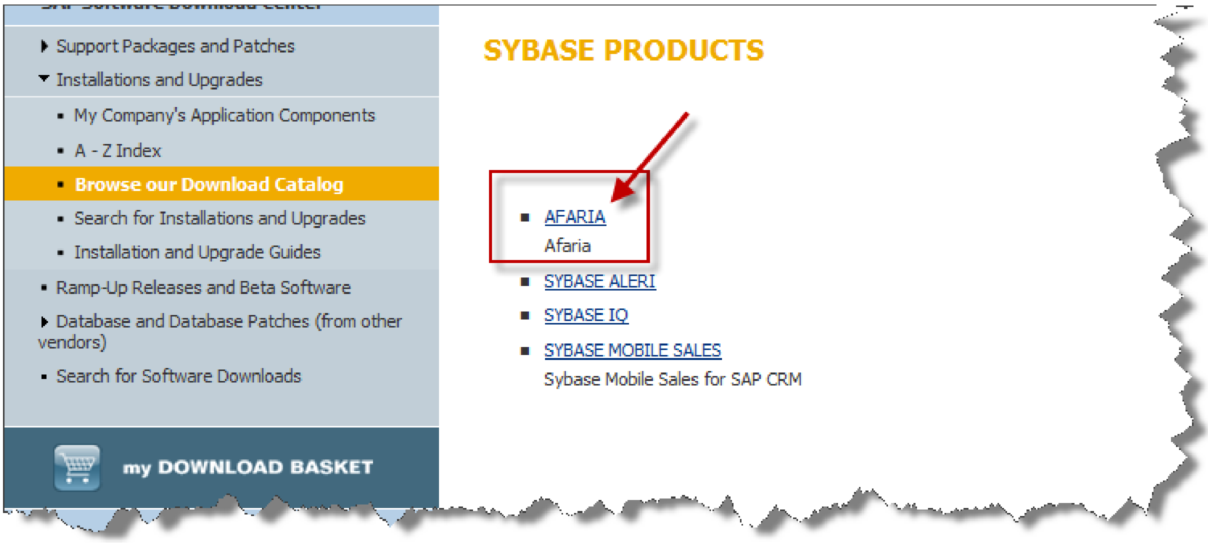
like SAP Plug-In, SAP Enterprise Portal Plug-In, SAP Solution Tools, ...

Supplementary Components for Cross Industry Solutions

like Project Management, Life-Cycle Data Management (SAP PLM Integrations), SAP Railcar Management, SAP Test Data Migration Server, SAP Visual Basis, ...

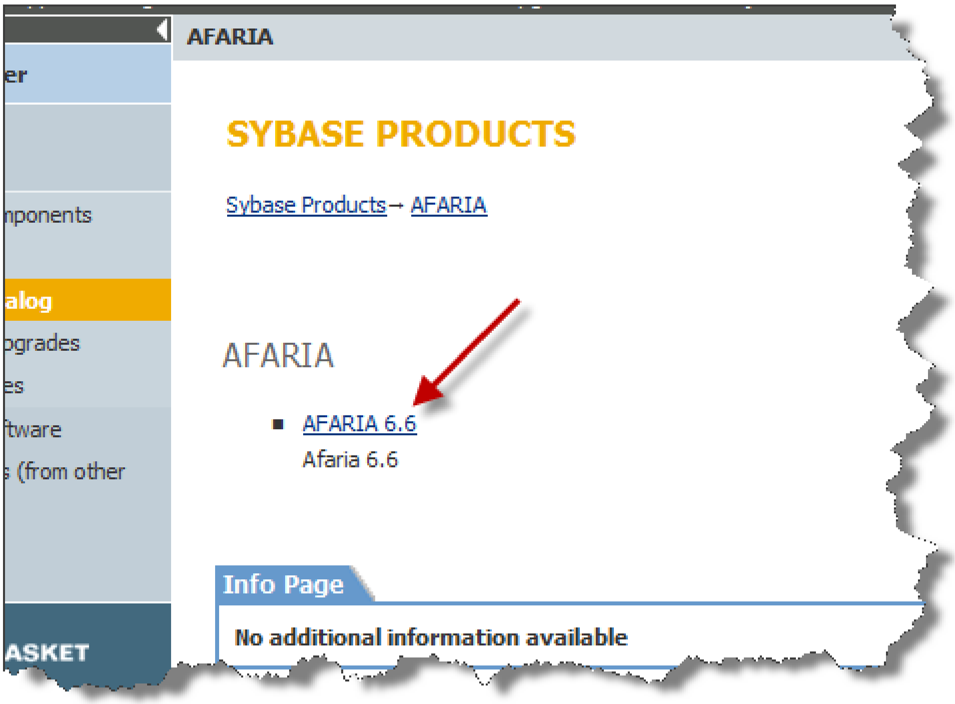
Sybase Products

like AFARIA, Sybase Mobile Sales, Sybase Mobile Workflow, Sybase Unwired Platform, ...


Support Packages and Patches
Installations and Upgrades
My Company's Application Components
A - Z Index
Browse our Download Catalog
Search for Installations and Upgrades
Installation and Upgrade Guides
Ramp-Up Releases and Beta Software
Database and Database Patches (from other vendors)
Search for Software Downloads
my DOWNLOAD BASKET

SYBASE PRODUCTS

- AFARIA
  Afaria
- SYBASE ALERI
- SYBASE IQ
- SYBASE MOBILE SALES
  Sybase Mobile Sales for SAP CRM



AFARIA

SYBASE PRODUCTS

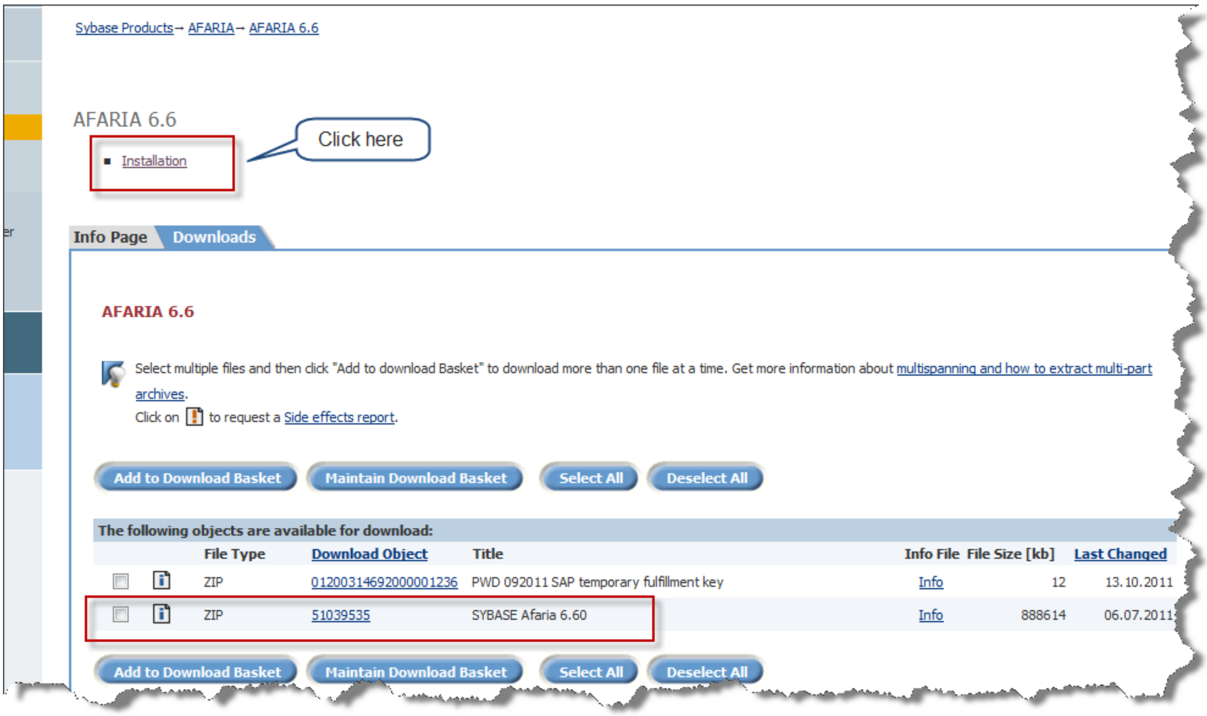
Sybase Products→ AFARIA

AFARIA

- AFARIA 6.6
  Afaria 6.6

Info Page

No additional information available



Sybase Products→ AFARIA→ AFARIA 6.6

AFARIA 6.6

- Installation

AFARIA 6.6

Select multiple files and then click "Add to download Basket" to download more than one file at a time. Get more information about multispanning and how to extract multi-part archives.

Click on ! to request a Side effects report.

The following objects are available for download:

		File Type	Download Object	Title	Info File	File Size [kb]	Last Changed
□	i	ZIP	01200314692000001236	PWD 092011 SAP temporary fulfillment key	Info	12	13.10.2011
□	i	ZIP	51039535	SYBASE Afaria 6.60	Info	888614	06.07.2011

Tip

Checks:

Has Afaria License been issued and available to use?

Has Software Media been downloaded with any latest updates released?

⚠ **CAUTION**

The download link may change and/or the procedure of obtaining the license key. Please check with your SAP contact for latest procedure in obtaining software as well as the license key.

3.2 Devices

Mobile devices, accordingly to the chosen device type(s) for the implementation, are to be made available and handy for the provisioning part. Depending on the device type, Afaria client application may need to be downloaded before provisioning from an applicable App Store or Marketplace.

Tip

Checks:

Are mobile devices available?

List Operating Systems of these devices (device types):

How many devices of each type?

No of Phones (e.g. iPhone) of each type:

No of Tablets (e.g. iPad) of each type:

Describe network type (e.g. 3G, Wi-Fi only, etc.):

3.3 OS User for Installation

A domain user will be required to perform the installations. The user has to be added in the local Adminstrator's group and UAC (User Access Control) settings to be turned off. This user requirement applies to both, Afaria and Relay Server in DMZ. The Relay Server may not have a domain user but a local Administrator user is must. The same user will be used to setup Afaria and Relay Server services during the installation.

This user needs to be created on both, Afaria and Relay Server, as mentioned above, added to server's local administrator user group with following attributes:

1. Password no expiration
2. Logon as Service

Tip

Checks:

Is Afaria service user created?

List the user name:

Is Relay Server service user created?

List the user name:

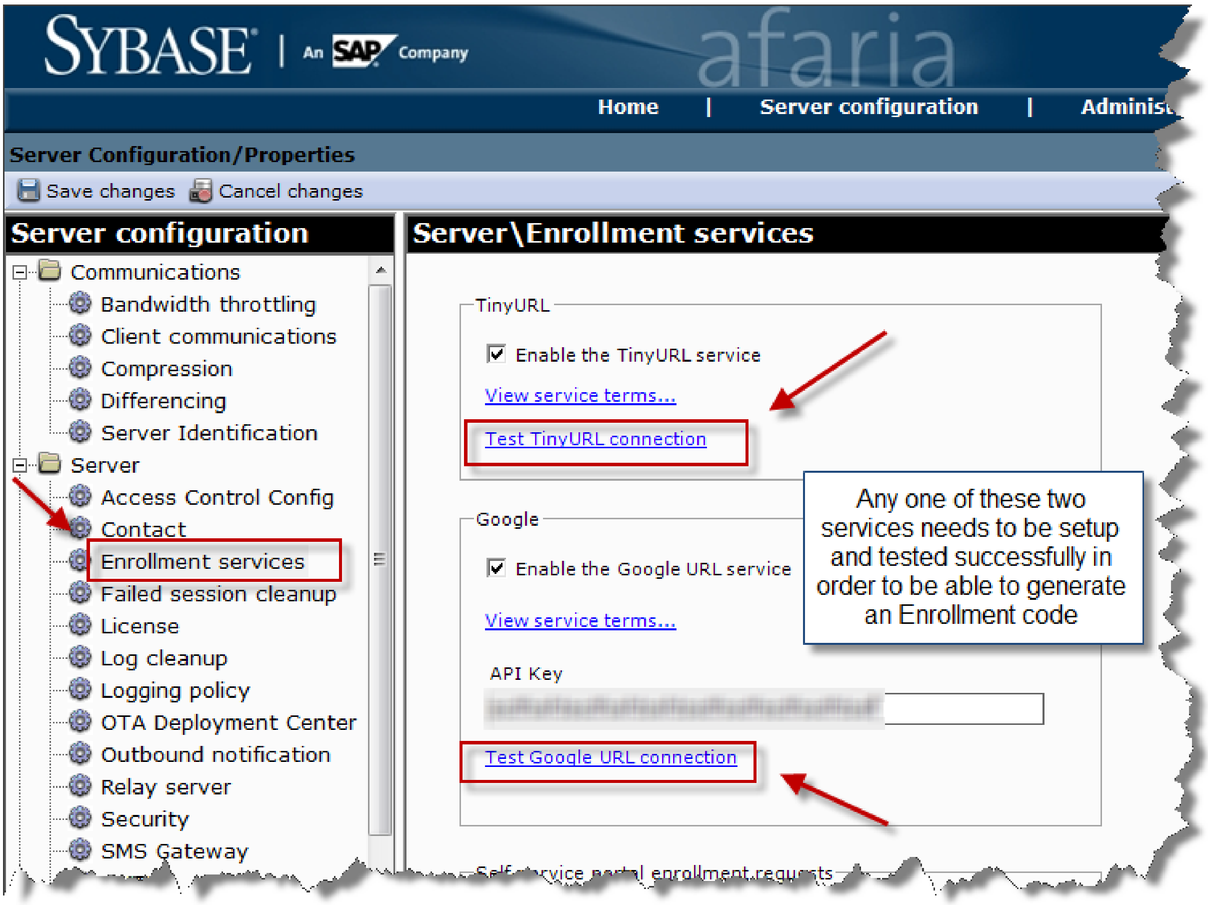
Password(s):

3.4 Internet Access

Internet access from Afaria and Relay Server is required for any missing patches; media download directly from SAP download site. Direct internet access from Afaria server needed for Enrollment Code procedure. In case of existing proxy layers the Afaria server to be included in the exceptions list.

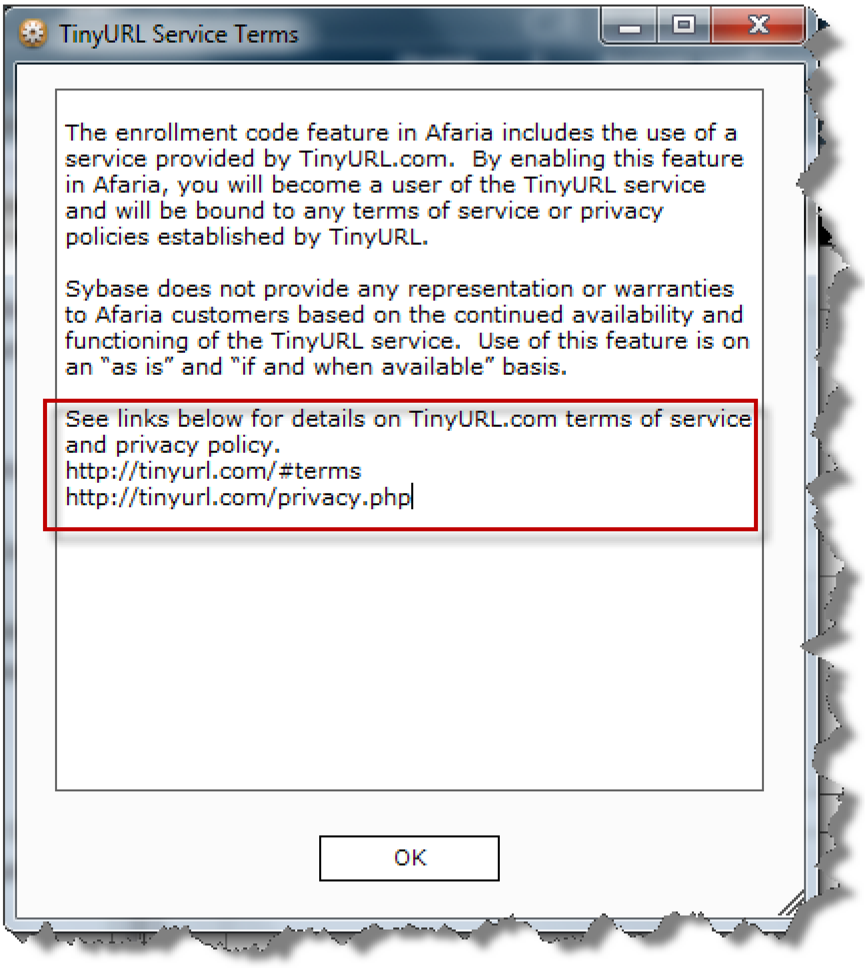
In-case if a Direct Internet access or an exception of the Afaria server is not possible, then as a work-around, addresses for TinyURL or Google's URL shortening service may need to be included in a 'white' or 'exception' list.

Test of either of the above mentioned URL shortening services will be performed on-site, in-case of an unsuccessful test the exceptions can then be made. The tests can be done from Afaria administrator's console as shown in the following screenshots.



Any one of these two services needs to be setup and tested successfully in order to be able to generate an Enrollment code

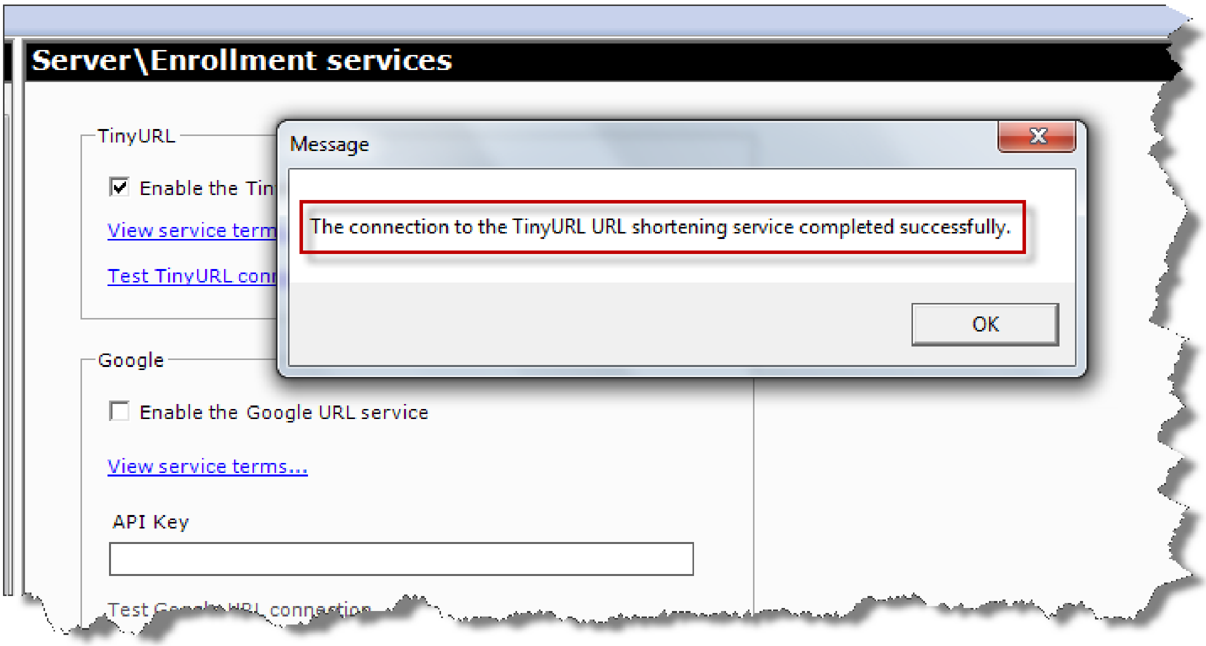
For TinyURL:



The enrollment code feature in Afaria includes the use of a service provided by TinyURL.com. By enabling this feature in Afaria, you will become a user of the TinyURL service and will be bound to any terms of service or privacy policies established by TinyURL.

Sybase does not provide any representation or warranties to Afaria customers based on the continued availability and functioning of the TinyURL service. Use of this feature is on an "as is" and "if and when available" basis.

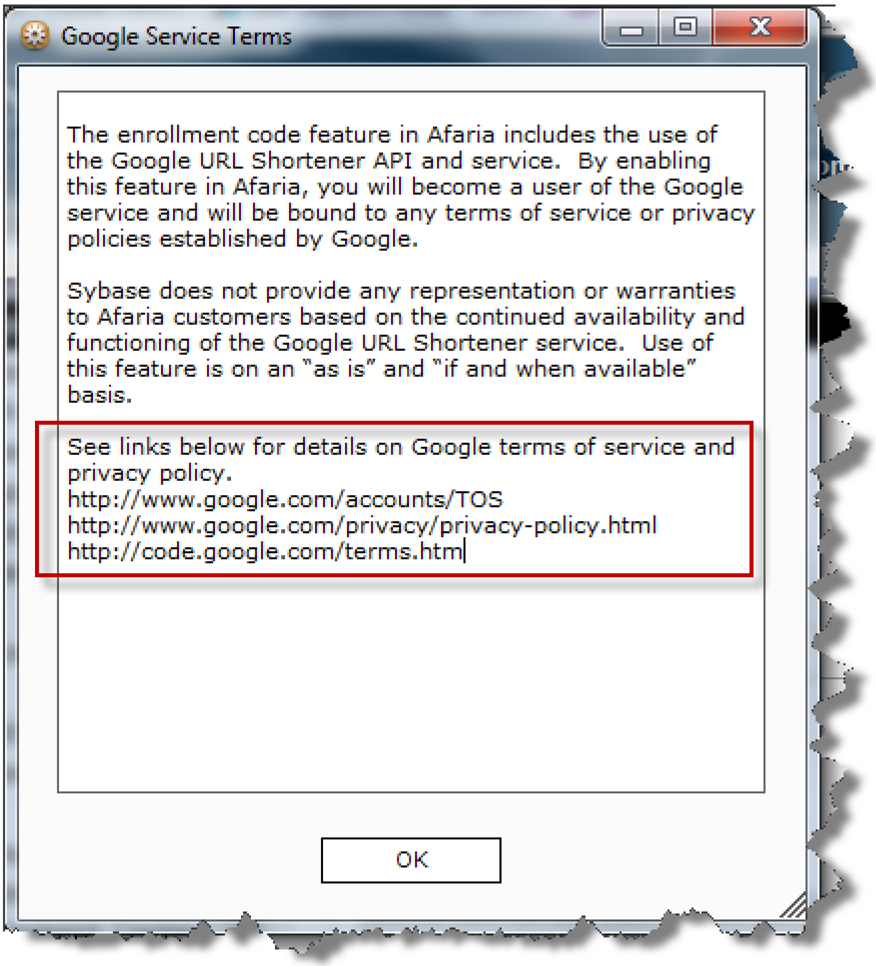
See links below for details on TinyURL.com terms of service and privacy policy.
http://tinyurl.com/#terms
http://tinyurl.com/privacy.php



Server\Enrollment services

The connection to the TinyURL URL shortening service completed successfully.

For Google's URL shortening service:



The enrollment code feature in Afaria includes the use of the Google URL Shortener API and service. By enabling this feature in Afaria, you will become a user of the Google service and will be bound to any terms of service or privacy policies established by Google.

Sybase does not provide any representation or warranties to Afaria customers based on the continued availability and functioning of the Google URL Shortener service. Use of this feature is on an "as is" and "if and when available" basis.

See links below for details on Google terms of service and privacy policy.
http://www.google.com/accounts/TOS
http://www.google.com/privacy/privacy-policy.html
http://code.google.com/terms.htm

Tip

Checks:

Is internet access available from Afaria server?

Is it a direct connection or by using proxy?

Is internet access available from Relay server?

Is it a direct connection or by using proxy?

Is internet access available for consultant?

3.5 Server Operating System

3.5.1 Afaria Server

Windows Server 2008 R2 (64 bit) Enterprise Edition

(To be able to add IIS and Active Directory Certificate Services Roles on the same server)

In case where an existing Enterprise CA is to be used, following are the alternate operating systems:

Any of the following Windows 64-bit operating systems:

Windows Server 2008 Standard Edition R2

Windows Server 2008 Enterprise Edition R2

Windows Server 2008 Datacenter Edition R2

Any of the following Windows 32-bit operating systems:

Windows Server 2003 Standard Edition R2

Windows Server 2003 Standard Edition with Service Pack 2

Windows Server 2003 Standard Edition with Service Pack 1

Windows Server 2003 Enterprise Edition R2

Windows Server 2003 Enterprise Edition with Service Pack 2

Windows Server 2003 Enterprise Edition with Service Pack 1

Recommendation

We recommend that you use Windows 2008 R2 (64 bit) Enterprise Edition.

We recommend that you install your operating system on NTFS rather than FAT32.

3.5.2 Relay Server in DMZ

Any of the following Windows 64-bit operating systems(RS v.12.0.1.3356):

- Windows Server 2008 Standard Edition R2
- Windows Server 2008 Enterprise Edition R2
- Windows Server 2008 Datacenter Edition R2
- Windows Server 2008 Web Server Edition R2

Any of the following Windows 32-bit operating systems:

- Windows Server 2003 Standard Edition R2
- Windows Server 2003 Standard Edition with Service Pack 2
- Windows Server 2003 Standard Edition with Service Pack 1
- Windows Server 2003 Enterprise Edition R2
- Windows Server 2003 Enterprise Edition with Service Pack 2
- Windows Server 2003 Enterprise Edition with Service Pack 1

Or

Apache on Linux OS [Apache (Linux 32 -bit only) RS v.12.0.1.3152]

This server in DMZ typically will have an external and an internal IP address setup so that the external devices can connect to this server from internet. In-case of having a single IP address, this server will need to be made reachable from internal server(s), e.g. Afaria server

This external IP address, mapped with the Relay Server host in DMZ, should be set functional in advance. In case of IIS, a typical test consultant may perform once IIS role is added to the relay server is to execute this external IP address in a web browser and launch standard IIS page.

Tip

Checks:

List the Server Operating System for Afaria Server:

List the Server Operating System for Relay Server:

Important

Determine if you are using a local CA for Afaria server or an existing Enterprise CA. The CA specific requirements can be found in the latest Release Notes as well as the Afaria installation guide.

3.6 Afaria Database

Afaria supports these databases in a production environment:

- iAnywhere SQL Anywhere® 11
- Microsoft SQL Server 2008 R2 Enterprise Edition
- Microsoft SQL Server 2008 R2 Standard Edition
- Microsoft SQL Server 2008 R2 Datacenter Edition
- Microsoft SQL Server 2008 R2 Parallel Data Warehouse Edition
- Microsoft SQL Server 2008 SP1 Enterprise Edition
- Microsoft SQL Server 2008 SP1 Standard Edition
- Microsoft SQL Server 2005 Enterprise Edition (SP1, SP2, SP3)
- Microsoft SQL Server 2005 Standard Edition (SP1, SP2, SP3)
- Oracle Database 11g Release
- Oracle Database 10g Release

Collations for Afaria operations - Afaria requires case insensitive collations, rather than binary collations, such as:

- (SQL Server 2008 R2) Latin1_General_CP1_CI_AS
- (SQL Server 2005) SQL_Latin1_General_CP1_CI_AS

Regional time zone – the Afaria database must be configured for the same time zone as the Afaria server components it supports.

Recommendation

We recommend installing Afaria Database on a separate server. While single server architecture can have Afaria server and the Database co-reside on the same server, We recommend it to be added to an existing SQL clustered environment or be installed separately on a different server.

3.6.1 Oracle Database Considerations

An Oracle database environment requires an Oracle client on each server component that accesses the database. Consider these items:

- Afaria server and Afaria Administrator require an Oracle client.
- If you are implementing iOS features the iOS provisioning server requires an Oracle client.

- If you are implementing iOS features, including the certificate authority (CA) server with the optional Afaria SCEP plug-in module, then the CA requires an Oracle client.
- Oracle server must use Oracle Provider for OLE DB.
- Oracle 10g and 11g clients are supported.
- On a server 64-bit operating system environment, install a 32-bit client with ODBC drivers and a 64-bit client with ODBC drivers.

Tip

Check:

List the chosen Database:

Recommendation

Refer latest Installation guide for specific steps for the chosen Database.

3.7 Hardware Requirements

3.7.1 Processor

Any of the following processor or compatible types:

- Intel Pentium 4 Processor processors at 2.0 GHz or higher
- Intel Core Duo, Intel Core Quad, Intel Core 2 Duo or Intel Core 2 Quad processors at 1.8 GHz or higher

The above is valid for both Afaria and Relay Servers.

Tip

Checks

List the processor for Afaria server:

List the processor for Relay server

3.7.2 Disk Space

3.7.2.1 Afaria Server

Minimum 40 GB free

3.7.2.2 Relay Server

Minimum 5 GB free

Tip

Checks

List the disk space available on Afaria server:

List the disk space available on Relay server:

3.8 RAM

3.8.1 Afaria Server

4 GB

Note

While the minimum RAM requirement is 1.5 GB in an environment where all individual components are installed on a separate servers, we recommend 4 GB RAM for a scenario where at least another Afaria component is installed on Afaria Server, e.g. Afaria Administrative Console.

3.8.2 Relay Server

2 GB

Tip

Checks:

List the memory available on Afaria server:

List the memory available on Relay server:

3.9 SMTP

Afaria server should be allowed to send out emails, i.e. SMTP server should allow Afaria server to send out emails. Following SMTP server information will be required:

1. SMTP server IP address;
2. User ID; and
3. Reply Address

Tip

Checks:

Is Afaria server allowed to send outbound emails using SMTP server?

List SMTP server name:

3.10 SSL – HTTPS

With iOS 5, Apple has a mandatory requirement that on the communication from the device to the first connecting system must be HTTPS with SSL enabled.

By using Relay Server, the first system for the device will be the Relay Server. In this case the Relay Server will need to be enabled with HTTPS using public IP or DNS.

Tasks, to accomplish the above, involve, once IIS is installed and Relay Server is primarily configured:

- Security team can install/configure customer specific SSL certificate(s) on the Relay Server host within IIS, such that the default IIS page can launch using HTTPS.
- To test the above execute the following using public IP or DNS of the Relay Server:
- https://<public DNS or IP of the Relay Server>
- The above should launch the IIS default page
- Once the default page is successfully launched using HTTPS (using presumably standard port 443), necessary configurations on the Afaria and Relay Server for it to work with iOS 5 can then be done.
- In case of Apache web server, the HTTPS requirements stay the same, by making sure that the default web page using HTTPS is launched successfully (It Works! Page for Apache).

Tip

Checks:

Are the security certificates created and on-hand to be able to launch the default IIS web page using HTTPS on Relay Server?

3.11 Apple ID

In case of iOS, end users will require to use Apple IDs and Password (establishing accounts with Apple) to download Afaria client application on the device.

The above requirement will also apply in-case of pushing and installing Apple App Store applications.

Tip

Checks:

Have the end test users setup Apple IDs to be able to download Afaria client application from Apple Application store?

3.12 Android C2DM

In case of Android Wi-Fi only devices, customer will need to sign up for Android Cloud to Device Messaging from the following link.
http://code.google.com/android/c2dm/signup.html

More information on the framework for the above can be found here:
http://code.google.com/android/c2dm/

Tip

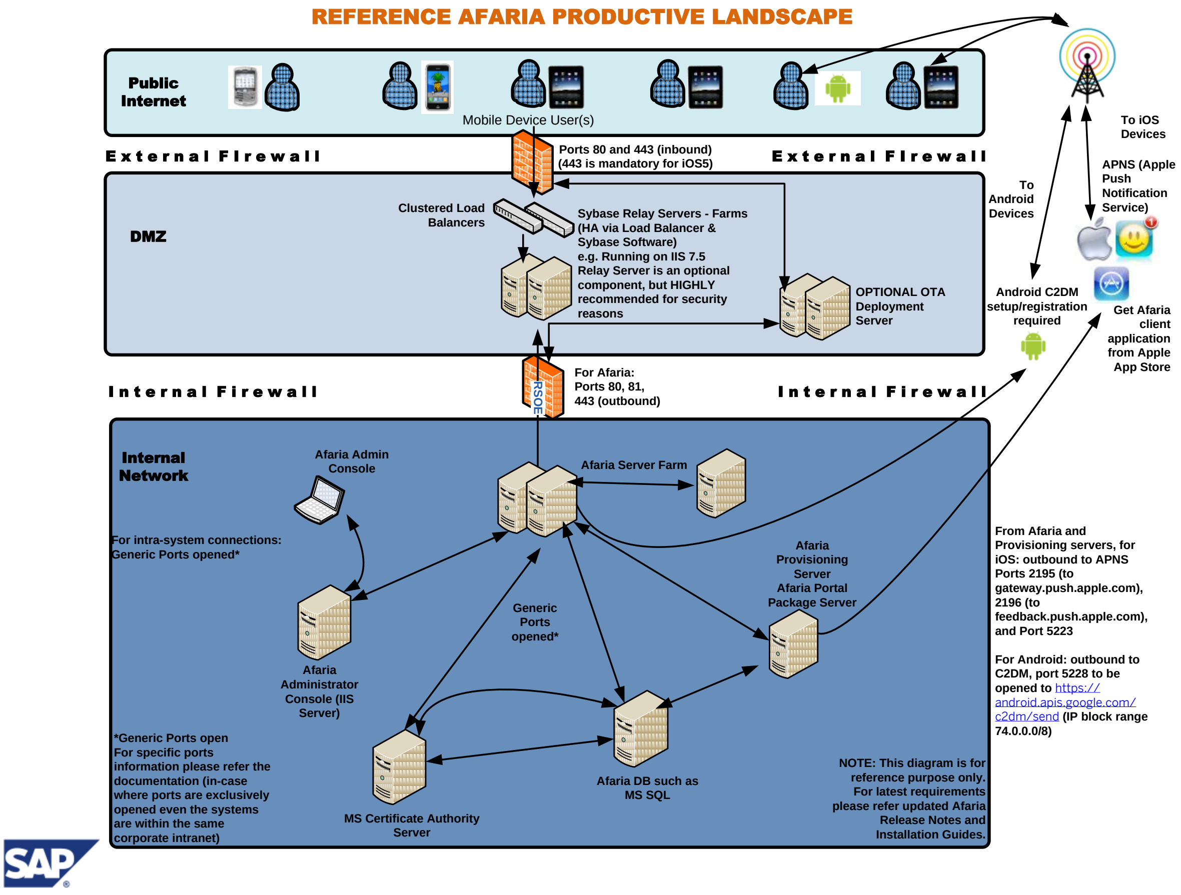
Checks:

Has a C2DM account been created?

What is the account ID?

3.13 Network Ports

For Afaria architecture to be able to function, certain ports need to be opened in the firewall. The details are as following. A sample diagram (not all inclusive but to give an overview of the port requirements) is also included below:


REFERENCE AFARIA PRODUCTIVE LANDSCAPE
Public Internet
Mobile Device User(s)
To iOS Devices
APNS (Apple Push Notification Service)
External Firewall
Ports 80 and 443 (inbound) (443 is mandatory for iOS5)
External Firewall
To Android Devices
DMZ
Clustered Load Balancers
Sybase Relay Servers - Farms (HA via Load Balancer & Sybase Software) e.g. Running on IIS 7.5 Relay Server is an optional component, but HIGHLY recommended for security reasons
OPTIONAL OTA Deployment Server
Android C2DM setup/registration required
Get Afaria client application from Apple App Store
Internal Firewall
RSOE
For Afaria: Ports 80, 81, 443 (outbound)
Internal Firewall
Internal Network
Afaria Admin Console
Afaria Server Farm
For intra-system connections: Generic Ports opened*
Afaria Provisioning Server Afaria Portal Package Server
Generic Ports opened*
Afaria Administrator Console (IIS Server)
*Generic Ports open For specific ports information please refer the documentation (in-case where ports are exclusively opened even the systems are within the same corporate intranet)
MS Certificate Authority Server
Afaria DB such as MS SQL
NOTE: This diagram is for reference purpose only. For latest requirements please refer updated Afaria Release Notes and Installation Guides.
From Afaria and Provisioning servers, for iOS: outbound to APNS Ports 2195 (to gateway.push.apple.com), 2196 (to feedback.push.apple.com), and Port 5223
For Android: outbound to C2DM, port 5228 to be opened to https://android.apis.google.com/c2dm/send (IP block range 74.0.0.0/8)
SAP

Ports that need to be opened:

- 80, 81, and 443 from Afaria to Relay Server **outbound**
- 80 and 443, from Public Internet to Relay Server **inbound**

3.13.1 iOS

- 2195 and 2196, and 5223 (5223 is used for Wi-Fi (only) devices) from Afaria server to Apple and from Devices to Internet (in case of Wi-Fi only devices to work within Corporate Wi-Fi) at gateway.push.apple.com and feedback.push.apple.com.
- These ports should be opened to the entire address block range as following, **Outbound**
  The IP address range for the push service is subject to change; the expectation is that providers will connect by hostname rather than IP address. The push service uses a load balancing scheme that yields a different IP address for the same hostname. However, the entire **17.0.0.0/8** address block is assigned to Apple, so you can specify that range in your firewall rules.

3.13.2 C2DM by Android

- Port 5228 to be opened outbound from Afaria server to: https://android.apis.google.com/c2dm/send

- This URL will resolve to different IP addresses, as of preparing this document Google hasn't published the IP range, thus requiring opening OUTBOUND to IP block 74.0.0.0/8.

- Port 5228 will also need to be opened outbound from any Wi-Fi network that a (particularly Wi-Fi only) device will use, either corporate or guest Wi-Fi network(s). The same address and IP range as above apply to this scenario.

> **Tip**
>
> Checks:
>
> List the ports opened to gateway.push.apple.com and feedback.push.apple.com, outbound:
>
> List the ports opened from Afaria server to Relay Server, outbound:
>
> List the ports opened from Internet to Relay Server, inbound:
>
> Has port 5228 been opened to Google directly from Afaria and corporate/guest Wi-Fi network(s)?

3.14 APNS by Apple

Apple rolled out a new process for customers to obtain APNs certificates for MDM without having to get developer licenses (http://www.apple.com/iphone/business/integration/mdm/).

This process requires the MDM vendor (i.e. Sybase/SAP for Afaria) to sign Certificate Signing Requests (CSRs) for each customer.

Current process is to create a ticket with support and send CSR to case owner by attaching the CSR to S2T2 (Sybase) or CSR to SAP message through Service Marketplace Instructions are in KB article 7779. Support will sign the CSR file and send it back to the customer.

> **Note**
>
> A webpage is being created to automate the process that will be accessed through the Sybase support site. Customer will sign in and upload the CSR file and then receive the signed CSR.

Tip

Checks:

Is signed CSR received?

Is an APNS certificate available, following the procedure in KB article # 7779?

(http://frontline.sybase.com/support/resolutionDetails.aspx?KBID=7779)

3.15 Apple Certificates

3.15.1 Procedure of Generating an APNS certificate

Generating an APNS Certificate on a Mac

1. On your Mac, navigate to Applications > Utilities > Keychain Access.
2. In the Menu bar at the top of the desktop window, choose Keychain Access > Certificate Assistant > Request a Certificate From a Certificate Authority.
3. In the Certificate Information window:
   a. In the User Email Address field, enter your email address.
   b. In the Common Name field, enter your name.
   c. In the "Request is" group, select the "Saved to disk" option.
   d. Select the "Let me specify key pair information" option.
4. Click continue.
5. For ease of access, choose your desktop as the location of the .CSR file.
6. In the Key Pair Information pane, choose 2048 as the key size and "RSA" as the algorithm.
7. Click Continue. The Certificate Assistant then saves the .CSR file to your desktop.

Generating an APNS Certificate on a Windows Server using IIS Manager

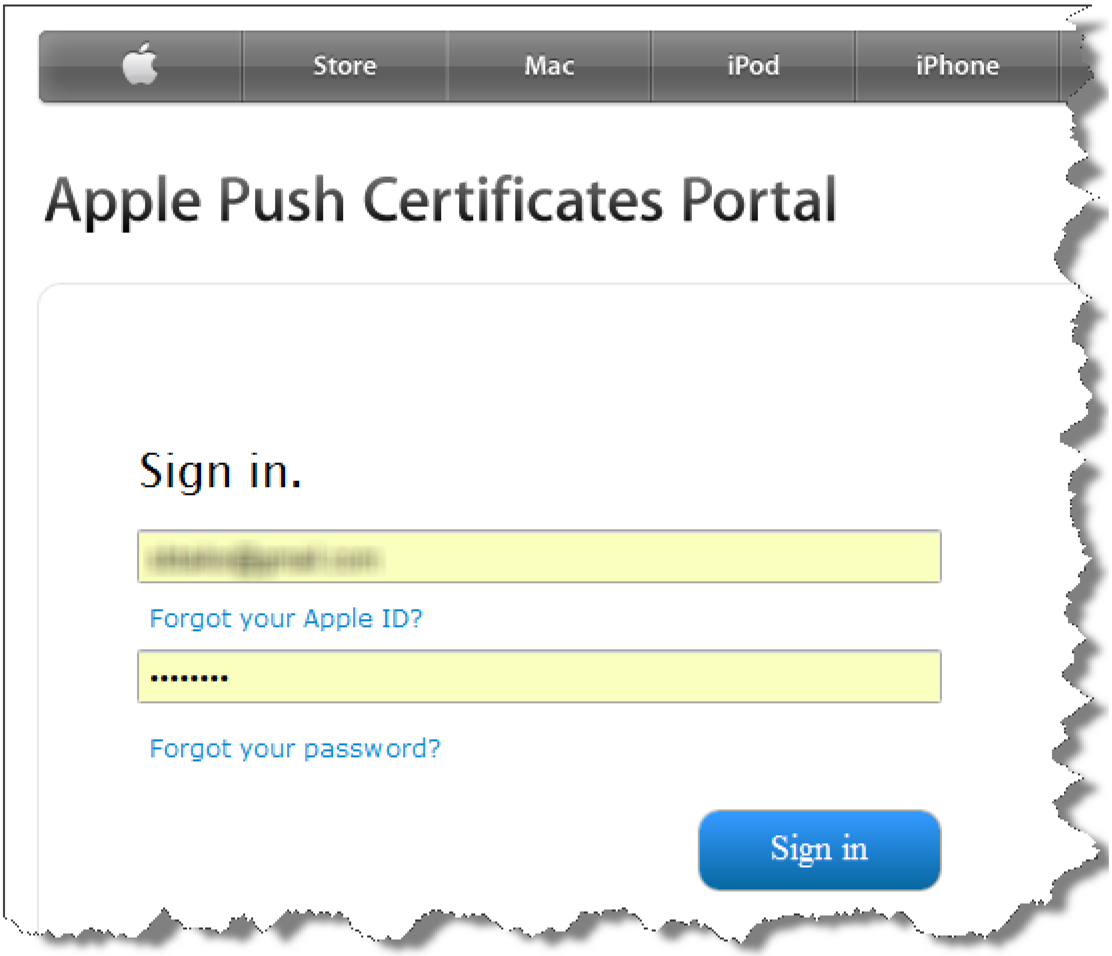
1. Click on the Start Menu, go to Administrative Tools, and click on Internet Information Services (IIS) Manager.
2. Click on the name of the server in the Connections column on the left.
3. Under the IIS section in the center window pane, double-click "Server Certificates"
4. In the Actions column on the right, click on Create Certificate Request…
5. On the Distinguished Name Properties window, enter the following information:
   a. Common Name – The name of the person generating the request (any name can be entered into this field).
   b. Organization – The legal name of your organization.
   c. Organizational Unit – The division of your organization handling the certificate (Most CAs don't validate this field).
   d. City/Locality – The city where your organization is located.
   e. State/province – The state/region where your organization is located.
   f. Country/Region – The two-letter ISO code for the country where your organization is located.
6. Leave the default Cryptographic Service Provider (Microsoft RSA…). Increase the Bit Length to 2048 or higher. Click Next.
7. Click the button with the three dots and enter a location and filename where you want to save the CSR file. Click Finish.

Send Certificate Signing Request (CSR) file to Sybase Support to be signed

1. Open a Technical Support case (either by calling 1-800-8SYBASE or online via case-express.sybase.com)
2. Customer provides the CSR file to case owner to be signed.
3. CSR file will be signed and the new, signed file will be a .SCSR (signed certificate signing request)
4. .SCSR file will be sent back to customer.

Upload SCRS file to Apple website and download APNS certificate

1. In a web browser (preferably Safari), go to the Apple Push Certificates Portal website: https://identity.apple.com/pushcert



2. Sign in using your Apple ID and password. (NOTE: This can be any valid Apple ID. This doesn't have to be an Apple ID associated with an Apple Developer Account.)
3. After you are logged in, select the "Create a Certificate" button.
4. Be sure to read the Terms of Use and accept the End User License Agreement.
5. Select the "Choose File" button to browse to the .SCSR file provided by Sybase.
6. Select the "Upload" button.
7. If successfully uploaded, the MDM certificate will be displayed on the "Certificates for Third-Party Servers" screen. (This screen is where all certificates issued under the logged in Apple ID will be displayed)
8. Select "Download" button to receive the Apple certificate. The obtained certificate will be in .pem format.

9. You can now log out of the Apple Push Certificates Portal.

Exporting the APNS Certificate to .pfx format

Important: You will need to ensure that you are installing the certificate on the same server that you generated the CSR on for successful association of the private key that was created during the CSR process.

A. Completing the CSR on a Mac and export the certificate

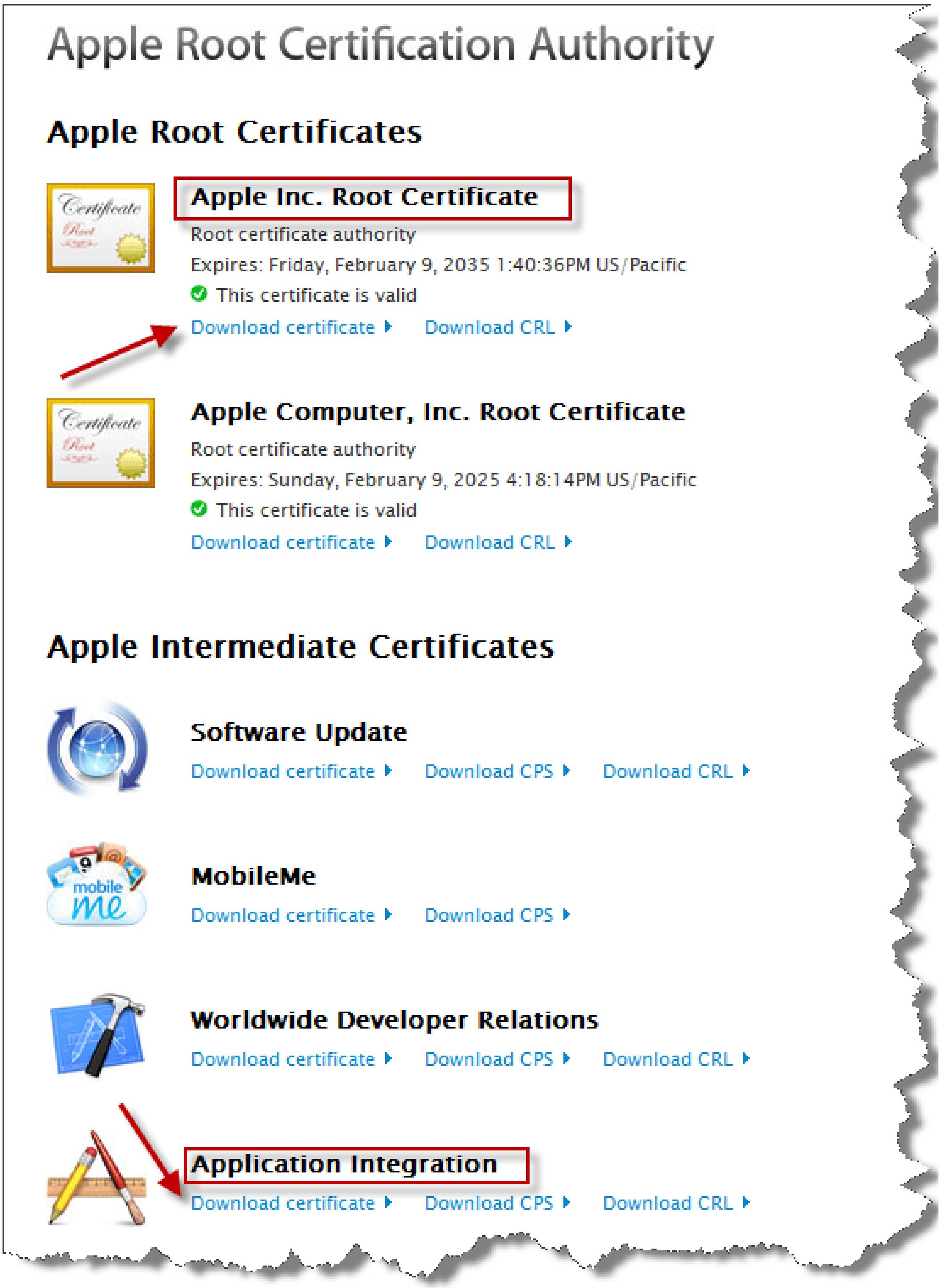
1. Copy the .pem certificate file to the Mac and double-click it to upload it to Keychain Access in order to complete the signing request.
2. In the Keychain Access window, select "Keys" in the left window pane under the Category section.
3. Expand the Name (the Common Name you entered when generating the CSR) that shows the "private key" under the Kind column.
4. Right-click the "APSP…" key and select Export…
5. Enter the password that you wish to set for exporting the certificate.
6. Now, you will have the certificate in .p12 or .pfx format.

B. Completing the CSR on a Windows Server using IIS Manager

1. Copy the .pem certificate file to the Windows Server.
2. Click on the Start Menu, go to Administrative Tools, and click on Internet Information Services (IIS) Manager.
3. Click on the name of the server in the Connections column on the left. Double-click on Server Certificates.
4. In the Actions column on the right, click on Complete Certificate Request…
5. Click the button with the three dots and select the .pem certificate that you received from the Apple Push Certificates Portal. If the certificate doesn't have a .cer file extension, select to view all types.
6. Enter a friendly name you want so you can keep track of the certificate on this server. Click OK.
7. If successful, you will see the certificate in the list. If you receive an error stating that the request or private key can't be found, make sure you are using the correct certificate and that you are installing it to the same server that you generated the CSR on.
8. Now, you need to export the APNS certificate to the correct format. Right-click the certificate you just imported and select Export.
9. Click the button with the three dots to specify a path to save the certificate file in .pfx format. When exporting the certificate, you are required to enter a password used for exporting the certificate.
10. Now, you will have the certificate in .pfx format.

Obtaining the additional Apple Root and Intermediate Certificates to be used with the new APNS Certificate

1. The new APNS certificate obtained from the Apple Push Certificates Portal requires a different Root and Intermediate certificate than the APNS certificate you obtain from the Apple Developer Portal. To obtain these new certificates, in a web browser, go to http://www.apple.com/certificateauthority
2. In the Apple Root Certificates section, download the "Apple Inc. Root Certificate".
3. In the Apple Intermediate Certificates section, download the "Application Integration (AAICA)" Certificate.



Apple Root Certification Authority

Apple Root Certificates

Apple Inc. Root Certificate

Root certificate authority

Expires: Friday, February 9, 2035 1:40:36PM US/Pacific

✓ This certificate is valid

Download certificate ▸ Download CRL ▸

Apple Computer, Inc. Root Certificate

Root certificate authority

Expires: Sunday, February 9, 2025 4:18:14PM US/Pacific

✓ This certificate is valid

Download certificate ▸ Download CRL ▸

Apple Intermediate Certificates

Software Update

Download certificate ▸ Download CPS ▸ Download CRL ▸

MobileMe

Download certificate ▸ Download CPS ▸

Worldwide Developer Relations

Download certificate ▸ Download CPS ▸ Download CRL ▸

Application Integration

Download certificate ▸ Download CPS ▸ Download CRL ▸

3.16 Installing the Apple Certificates on the Afaria Server Farm Master

3.16.1 Certificates needed:

a. Apple Inc. Root Certificate (.cer file)
b. Apple Integration (AAICA) Certificate (.cer file)
c. APSP… push certificate (.pfx or .p12 file)

3.16.2 Instructions for installing the certificates on the Afaria Server:

1. Browse to <ServerInstallationDirectory>\bin\InstallPushCert.exe.
2. Right-click and select "Run as administrator".
3. Browse to each of the required certificates.
4. Enter the correct password required for exporting the Push certificate.
5. Leave the "Modify ACL" checkbox selected.
6. Click Install.
7. Verify the pop-up dialog indicates success.

3.16.3 Alternate Instructions for installing the certificates on the Afaria Server:

1. Create a MMC snap-in for Certificate
    a. Launch MMC console (Start > Run > MMC)
    b. Add snap-in for certificates (select "Computer account" for type of certificate)
2. Add Root and AAICA certificates as trusted root certificates
    a. Launch MMC console
    b. Select Certificates > Trusted Root Certification Authorities > Certificates
    c. Import Apple, Inc. Root Certificate
    d. Import Application Integration (AAICA) certificate
3. Add APNS certificate as personal certificate
    a. Launch MMC console
    b. Select Certificates > Personal > Certificates
    c. Import Apple Push Notification Certificate (.pfx or .p12 file)
4. Add APNS certificate name to Afaria configuration
    a. Launch the Afaria Administrator web UI
    b. Go to Server Configuration > Properties > iOS Configuration
    c. On a 2011_04 and earlier Server, select "Browse" to choose the Apple Push Notification Certificate you just imported to the Personal Certificate Store.
    d. On a 2011_05 Server, select "Install Certificate…" and browse to the file location of the Apple Push Notification Certificate (.p12 or .pfx file) you exported.

4. Appendix

Following is some additional useful information in setting up the environment:

> ⚠ **CAUTION**
>
> Please refer to the latest release notes for up-to-date information. The information below may change and updated via release notes. Here is the direct links to the relevant release notes:
>
> Afaria Release Notes and System Requirements
> http://frontline.sybase.com/support/fileDownload.aspx?ID=2260
>
> Afaria Support Documentation
> http://frontline.sybase.com/support/documents.aspx

4.1 Certificate Authority (CA)

Afaria iOS features require a Microsoft CA as part of the implementation, regardless of whether you include optional iOS payload signing or optional secure connections as part of your enterprise's Afaria iOS implementation.

Consult your Microsoft documentation resources to learn how to set up your CA to comply with the following requirements.

	Requirements
Operating System	• Microsoft Windows Server 2008 Enterprise or Windows Server 2008 R2 Enterprise with: o IIS o Active Directory Certificate Services role • Microsoft Windows Server 2003 Enterprise[1] with: o IIS o Active Directory Certificate Services role o Simple Certificate Enrollment Protocol (SCEP) Add-on for Certificate Services, as distributed by Microsoft, Inc. with the following considerations: ▪ Install using a local user account with administrative privileges. ▪ During the installation, choose to enable the challenge phrase option. The option is enabled by default and is recommended for security. See the *Installing Afaria* guide for information about configuring your CA. Refer to your Microsoft Windows Server and Microsoft Server Manager (administrative tool) product documentation to learn about adding roles, using the New Role Wizard, and the Active Directory Certificate Services (AD CS) role.

Additional requirements	• iOS devices require verification of the complete chain of trust. Ensure that the entire authority chain is online for iOS device connections. • The identity credentials used for CA's IIS SCEP application pool must match the credentials on the Provisioning Server configuration page on the Afaria server. • For embedding a SCEP request in an Afaria Device Configuration policy for Wi-Fi or VPN, only a Windows Server 2008 or Windows Server 2008 R2 certificate authority is supported. • The Afaria SCEP plug-in is available in 32- and 64-bit versions and are designed to run on operating systems with the same bit level. • Microsoft's SCEP add-on for Windows Server 2003 is not available in a 64-bit version. Therefore, installing the Afaria SCEP plug-in on a Windows Server 2003 64-bit server is not supported.
Database	• The server must be configured for the same time zone as the database server. • (With Afaria SCEP plug-in module) For Oracle database, the server requires an Oracle client. Use the Net Configuration Assistant to create a local net service with the same name as you created for the Afaria server.
Relay Server	Supported
Connectivity	• (Without Afaria SCEP plug-in module) The server does not require connectivity to any Afaria component server. • (With Afaria SCEP plug-in module) Outbound port – the server requires outbound connectivity to the Afaria database, which is configurable for each supported database type. • (With Relay Server) Outbound port 80 (HTTP) or 443 (HTTPS) – if the Relay Server Outbound Enabler (RSOE, rsoe.exe) is resident on the server, the server uses the ports to connect to the Relay Server. If the RSOE resides on a different server, the server uses the ports to connect to the RSOE. • (Without Relay Server) Outbound port 80 (HTTP) or 443 (HTTPS) – the server uses the port to reply to clients. • Devices require connectivity to the server or its optional relay server proxy. Connectivity requirements can be met by database credentials, same-domain residency, cross-domain trusting, or a shared workgroup, as appropriate for your enterprise environment.
For Reference	The Microsoft SCEP Implementation White Paper – www.microsoft.com/download/en/details.aspx?id=1607

[1] A Microsoft Windows Server 2003 certificate authority environment does not support issuing Afaria Device Configuration policies of type "SCEP."

4.2 Component and Feature Requirements – Relay Server

The Sybase iAnywhere Relay Server is a secure, load-balanced proxy server that relays communication between mobile devices and one or more Sybase server-based products. It is developed independently from Afaria. Afaria is one example of a supported product.

Relay Server is an optional component that is bundled with the Afaria product on the product installation image. For your convenience, updates to Relay Server may be available on the technical support site.

See *Installing Afaria > Setting Up the Relay Server* for installation instructions. The technical support site knowledge base also contains articles about installing and operating the relay server in the Afaria environment.

	Requirements
Relay Server	• 12.0.1 • 11.0.1
Web Server	• IIS 7.5 or 6.0 on Windows OS • Apache on Linux OS
Afaria Server Components	Afaria supports using relay server for connections to these Afaria server components: • Afaria server, as used for device connections or Afaria Access Control for Email connections • Afaria provisioning server • Afaria portal package server • Certificate authority for Afaria operations • OMA DM server
Additional Requirements	• All Relay Server Outbound Enabler (rsoe.exe) instances in Afaria must be the same version. Afaria uses rsoe.exe in these locations: o (Afaria core operations, Access Control for Email) Afaria server – <ServerInstallDirectory>\bin\RSOutboundEnabler\ o (iOS features) iOS provisioning server – user-defined o (iOS features) Certificate Authority – user-defined o (OMA DM) OMA DM server – user-defined o (Portal Package) Portal Package server – user-defined • At the time of the Afaria 6.6 release, server requirements are[1]: o Windows or Linux x86/x64[2]. o Relay Server on IIS may coexist with other IIS applications. ▪ Relay Server may coexist with other virtual Web server under the same IIS install. ▪ Relay Server may coexist with other Web site (or directory) under the same logical Web server. ▪ Relay Server Web server extensions may coexist with other Web server extensions sharing the same application pool. However, application pool properties are then limited to being Relay Server

	compatible (in general, all worker recycling options need to be turned off).

[1] Relay server 11.0 requirements, as a component of the SQL Anywhere 11.0.1 product release, are available at www.sybase.com/detail?id=1002288 (search for "Relay Server"). Relay server 12.0 requirements, as a component of the SQL Anywhere 12.0.0 product release, are available at www.sybase.com/detail?id=1089646.

[2] Linux on an x64 system supports only 32-bit relay server components.

4.3 Client Requirements – iOS

	Requirements for Client
Operating System	On iPhone, iTouch, iPad, and iPad 2 devices: • iOS 5[1] • iOS 4.3, 4.2, 4.1, 4.0 • iOS 3.2.2[2] 3.1.3
Upgrade Method	To upgrade a client that is under Afaria Mobile Device Management (MDM) control, connect to an upgraded server. To upgrade a client's installed agent, install an update from the Apple App Store.
Protocol Support	HTTP, HTTPS
Core Features	Access Control for Email Authentication, server Client notification to connect Data views, custom Groups, dynamic Groups, static OTA provisioning Relay server Remote wipe/device lock
Policies and Portal Packages	Device Configuration[3] Portal Application Packages[4]
Components	Configuration Manager Inventory Manager

[1] Once enrolled in Afaria MDM control, iOS 5 devices require HTTPS on all connections. The secure connection can occur either at the optional relay server or the provisioning server.

[2] iOS 3.x does not report its serial number for Afaria inventory collection.

[3] A Microsoft Windows Server 2003 certificate authority environment does not support issuing Afaria Device Configuration policies of type "SCEP."

[4] For iOS 4.x, enterprise and commercial applications are supported. For iOS 3.x, only commercial applications are supported.

4.4 Client Requirements – BlackBerry

	Requirements for Basic Client[1]
Operating System	• 6 • 5
Desktop Synchronization	N/A
Upgrade Method	Connect to upgraded server.
Protocol support	XNET, XNETS, HTTP, HTTPS
	Advisory for SSL (XNETS, HTTPS) and schedule monitors – Secure connections require user interaction to negotiate the communication handshake. The device prompts the user to enter a portion of the certificate's thumbprint. This has particular implications when using an Afaria schedule monitor paired with an action that establishes a connection; an action intended to execute without user intervention. The connection cannot run unattended because making the connection requires user input.
Core Features	Authentication, client[2] Authentication, server Client notification to connect Data views, custom Groups, dynamic Groups, static Monitor, schedule OTA deployment Relay server Remote wipe/device lock
Components	Inventory Manager[3] License Manager[4] Session Manager

	Additional Requirements for Features and Components
Client Notification to Connect	Short Message Service (SMS) Data service

[1] This feature is not supported or available for double-byte character environments.

[2] The BlackBerry platform requires users to interact with their device to facilitate client authentication. Test devices in your environment to understand the user requirements.

[3] Inventory Manager change detection is not supported.

[4] This feature is not supported in multitenant environments.

4.5 Client Requirements – Android

	Requirements for Client
Operating System	• Afaria agent – named com.afaria.client, as created by the Afaria Create Client Installation program or installed from the Google Android Market, for Android OS phones and tablets: ○ 3.1 ○ 3.0 ○ 2.3 ○ 2.2[1] • Afaria Samsung agent – named com.afaria.client.samsungclient, as installed from the Samsung Apps store or the Google Android Market, for Android OS phones and tablets: ○ 2.3 with Afaria Advanced Enterprise Security for Samsung devices ○ 2.2[1] Afaria agents may be released to different markets at different times.
Upgrade Method	• For agents created by the Afaria Create Client Installation program, remove current agent, then install new agent. • For agents installed from the Samsung Apps store or the Google Android Market, install a new agent from the market.
Protocol Support	XNET, XNETS, HTTP, HTTPS
Core Features	Access Control for Email Client notification to connect Data views, custom Groups, dynamic Groups, static OTA provisioning Relay server Remote wipe/device lock
Policies and Portal Packages	Portal Application Packages
Components	Configuration Manager Inventory Manager[2] License Manager Session Manager
Cloud to Device	• Device is enabled for Google services by having an active Google account on the device.

Messaging (C2DM)	• (Devices using Wi-Fi) Outbound port 5228 - port must be open for Google services traffic, including C2DM push notifications.

[1] Update 2.2.20.A955.Verizon.en.UK – due to a known issue with the update's security features, this update is not supported for Afaria's security features, such as device lock, unlock, and password enforcement. See www.droidforums.net.

[2] Inventory Manager change detection is not supported.

	Additional Requirements for Features and Components
Configuration Manager	• NitroDesk TouchDown features ○ Component licensing – you are licensed for both Configuration Manager and Inventory Manager. ○ Android NitroDesk TouchDown client – must be compatible with the Afaria product. ▪ TouchDown client version 6.4 is required, currently available on the Android Market. ▪ Uninstall any other TouchDown client instance before installing the required client. ▪ To manage TouchDown client with Afaria Access Control for Email, use Afaria to configure the TouchDown client. Otherwise, the device is always assigned the unknown device policy. ○ Client data wipe - the wipe capability is enabled for an Android NitroDesk TouchDown client only after the client's software inventory is reported to the Afaria server. • Samsung Advanced Enterprise Security (AES) features ○ Supported only on Samsung devices that support enterprise mobile device management (MDM), as first introduced with the Android 2.3.3 Galaxy S II device. ○ Configuration Manager > Android > Samsung channels created prior to Afaria 6.6 FP1 2011_03 hot fix Af66Fx18 are not compatible with hot fix Af66Fx18 or later versions. • Motorola features – Motorola devices that support enterprise device management, as first introduced with the anticipated Droid Pro.

4.6 Antivirus, known Applications, and OS features

The below processes have been known to affect the ability for Afaria to function correctly:

Microsoft's Data Execution Prevention (DEP)

- Afaria is not programmed to be 100% with the Microsoft DEP feature on Windows XP SP2 or Windows Server 2003 SP1 and later operating systems.

Antivirus software real-time or on-access type scanning and Scheduled scans

- Afaria is very file intensive when modifying Channels and during Channel Replication. All the Channels for Replication and inbound client connections are accessed constantly; especially in high load environments. Real-time or On-Access type Antivirus scanning scanning can cause timing issues, error messages, and has even been known to corrupt channels during operation.

- Scheduled scans that coincide with system operations, examples of these include, but are not limited to Channel Replication, Client Group Refresh and modification of Channel/Profile objects, which have the potential to become corrupt for the same reasons listed above.

Connectivity issues exist between the Afaria Server(s) and the Afaria database server

- If and Afaria Server looses the connection to the Afaria database, the Afaria Server Service will stop and possibly trap in certain scenarios.

Backup software

- Afaria is very file intensive when modifying Channels and during Channel Replication. All the Channels for Replication and inbound client connections are accessed constantly; especially in high load environments. The use of the Afaria Administrator to modify any Channels or to initiate a Channel Replication manually AND scheduled Channel Replication must not occur when a Backup is being performed. Backups while the Afaria Server Service is started has been known to cause file locking, corruption, etc.

File contention/ file locking that may be caused by another application attempting use the same file that is being transferred

MORE INFORMATION:
The following numbered solutions correspond to the above list of potential causes.

1. Microsoft's DEP feature is enabled for all programs and services. Afaria will not function properly with DEP enabled. If DEP is required to run on your Afaria systems, you have two options:

- Preferably, select the option "Turn on DEP for essential Windows programs and services only".
- If necessary, you can select the option "Turn on DEP for all programs ans services except those I select" but you must exclude all executables (EXE files) within the Afaria Server and Afaria Administrator program directories (installation paths).
- Additional information about Microsoft's DEP feature can be reviewed http://support.microsoft.com/kb/875352.

2. If Antivirus software has Real-Time/On-Access or scheduled scans enabled, exclude the the Afaria Server and Afaria Administrator installation directories (*.* and all subdirectories) from these types of scans.

- If you are using an enterprise policy agent (e.g. McAfee EPO) for anti-virus management, you must update the policy or the local changes will be overwritten when the policy is applied later.
- Additionally exclude the ,safe and ,pre file extensions. These are the file extensions that Afaria uses for safe file transfer feature.

3. Afaria is unable to communicate appropriately with the database server. The database server may have been rebooted or the network link removed. Transaction Log or Data Log files may be excessively large or database growth may be restricted. Try any or all of the following and then attempt Client connections:

- Stop and restart the Afaria services.
- Verify that the SQL database has "Truncate Log on Checkpoint" enabled or Recovery Model set to Simple.
- Verify that the size of the Afaria database transaction log file and data log file are not restricted either by database properties or limited disk volume.
- If a domain controller is in use, reboot it.

4. Backup software could be running and locking the source files accessed by the File Transfer events. Backups should not be enabled while the Afaria Server is running.
5. There may be file contention on the source files accessed by the File Transfer events. It may be necessary to create a temporary copy of the source file prior to sending it to the Client. This will require additional disk space.

5. References

Frontline web-site of Sybase:

http://frontline.sybase.com

What is the process to follow in order to generate a APNS certificate from the Apple Push Certificates Portal?

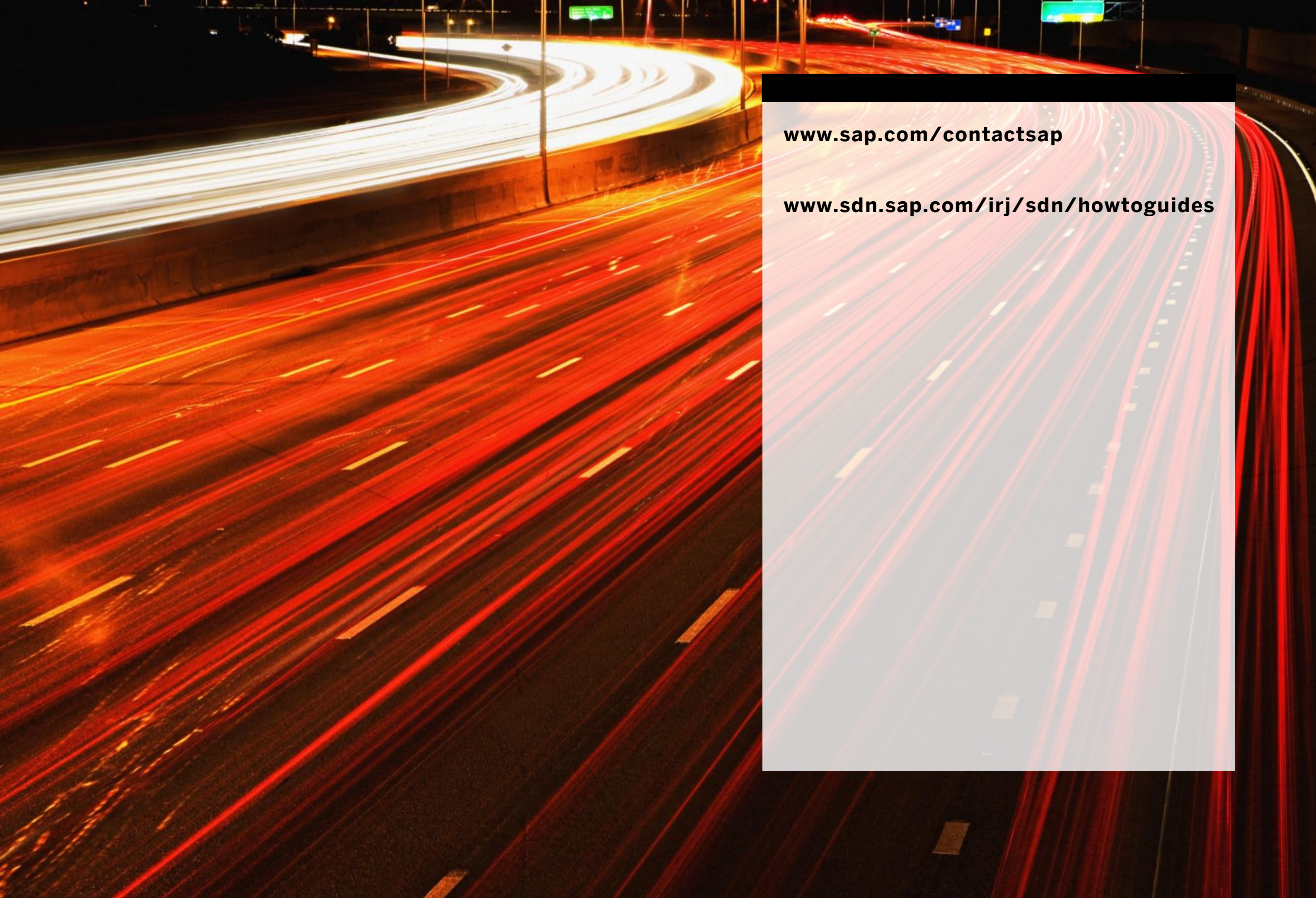
KB Article # 7779

http://frontline.sybase.com/support/resolutionDetails.aspx?KBID=7779

Are there any known applications or operating system features that can conflict with the proper operation of Afaria?

KB Article # 5042

http://frontline.sybase.com/support/resolutionDetails.aspx?KBID=5042



www.sap.com/contactsap

www.sdn.sap.com/irj/sdn/howtoguides

The Best-Run Businesses Run SAP™