

Using the Afaria® Trial Virtual Machine

Sybase® iAnywhere's Afaria has been built from the ground up to address the unique challenges of frontline environments. It provides comprehensive capabilities to proactively manage and secure all the devices, applications, data and communications critical to frontline success, regardless of the bandwidth available. Afaria provides high reliability and simple usability for mobile device users, thereby increasing user adoption. For the administrator, Afaria is an enterprise-grade, highly scalable solution with a central web-based console that allows you to control a host of key functions from a standard browser. With Afaria's ability to integrate with enterprise directories, these functions provide everything necessary to extend an organization's management and security capabilities to any device, in any location.

Using the Afaria Trial Virtual Machine instructs the trial administrator on how proceed once the Afaria trial virtual machine (VM) image is installed. It includes a tour of the environment, an overview of the trial licensing, some "Do's" and "Don'ts", and guidance on using the Afaria product in this virtual machine context. You can use this trial to find out firsthand how you can use Afaria to face the challenge of securely managing computing devices at the front lines of the business enterprise.

Table of Contents

Before you begin.....	3
Document conventions	3
Afaria trial news group	3
Afaria sales and information	3
Afaria Client requirements	5
Start the VM and log on	6
VM desktop	7
Afaria Administrator tour	8
Sample inventory scans	9
Afaria trial VM Do's and Don'ts	10
Afaria features and Clients.....	11
Component and feature Client support	12
Creating, deploying, and configuring the Afaria Client	15
Predefined profiles and channels.....	17
Case study: Acme, Inc.	17

Before you begin

This guide introduces you to the Afaria trial virtual machine. Using Acrobat Reader's hyperlinks and Find feature make this guide easy to use online.

Document conventions



This graphic presents a note about the preceding paragraph.



This graphic presents information that is critical to a successful trial.

Please contact us with feedback or questions about your Afaria trial experience.

Afaria trial news group

Please contact us with feedback or questions about your Afaria trial experience. Use the news group to discuss your experience, ask questions, and report any issues you encounter.

News group on Sybase.com — www.sybase.com/detail?id=1050798

Afaria sales and information

Contact your regional marketing team for Afaria product information and sales.

Asia-Pacific

- Phone — +852 2506 8700

EMEA Germany

- Phone — +49 (0) 7032 798-0
- Email — info_ias_germany@sybase.com

EMEA UK

- Phone — +44 (1) 628 597100
- Email — ukinfo@sybase.com

Japan

- Phone — +81 3 5544 6400
- Email — ias_mktg_jp@ianywhere.com

North America

- Phone — 800-8SYBASE
- Phone — 519-883-6898
- Email — contact_us@ianywhere.com



Afaria Client requirements



You must ensure that your test devices meet the requirements for Afaria Clients. Devices that deviate from the stated Client requirements may perform in unpredictable and undesirable ways.

Verify that the computing devices you plan to use with this trial meet the Afaria Client system requirements, as cited on www.sybase.com/products/mobileenterprise/afaria/system-requirements. The requirements are abbreviated and stated in general terms on the web page. Therefore, please verify your devices against the complete list of Client requirements that is available as a download (.CHM) from the same page. Ideally, you should use test devices that you can reset during or after the trial.

Start the VM and log on

Start the trial's VM by selecting it in the Virtual PC Console list and choosing Start. Allow time for the boot process and log on.

- VM commands — Commands are available in the window's Action menu. Use the Action menu to deliver the “CTRL-ALT-DEL” key sequence or use the alternate key sequence “Right ALT + DEL” to log on.
- Case-sensitive user credentials — User name = Administrator, Password = Evaluation1.
- About Windows dialog — Microsoft is represented by the About Windows dialog presented on the desktop.
- Select Your Region/End-User License Agreement dialog — Microsoft and Sybase are both represented by the license agreement presented on the desktop. You can proceed with the trial only after accepting the license agreement. You can reboot the VM to receive the license agreement again if you accidentally decline and would like another opportunity to accept.

VM desktop

The VM desktop includes the following items that are associated with the trial VM and Afaria operations.

- “Afaria Administrator” IE shortcut — Starts the Afaria Administrator application.
- “Afaria trial VM – Start here” folder — Includes the following introductory documents and navigational shortcuts:
 - “Using the Afaria Trial Virtual Machine” (Using Afaria trial VM.PDF) — This document includes guidance for using the Afaria trial VM.
 - “Getting to Know Afaria” (GettingtoKnowAfaria.PDF) — This document is an excellent start for Afaria VM trial users, as it presents an overview of the Afaria architecture and an introduction to user interface features. It discusses Afaria Server configuration, creating and deploying Afaria Client software to computing devices, and using channel components such as Inventory Manager to create channels to run when an Afaria Client connects to the Server.
 - “Afaria documents” shortcut — Shortcut to the folder that holds the complete suite of Afaria product documentation. The folder includes subfolders for translation languages. All documents are available in English. Only select documents are available for other languages.
 - “Afaria Client Install Kits” shortcut — Shortcut to the folder that holds one predefined Afaria Client for each Client type. Each Client has an associated document file that contains a summary of the Client installation options used to create the Client.
 - “Afaria Inventory Scans” shortcut — Shortcut to the folder that hold numerous sample Inventory Manager inventory scans. Refer to [“Sample inventory scans” on page 9](#) for additional information on using the scans.
 - “IIS Server ISAPI filter” shortcut — Installation of the ISAPI filter is required only for customers who want to use the Afaria Access Control for Microsoft Exchange feature. Complete information and installation instructions can be found in the “Afaria 6.0 Reference Documentation”.
 - “Relay Server” shortcut — Installation of the Afaria Relay Server is required only for customers who want to use the Afaria Trial and wish to test the security features of the Afaria DMZ Relay Server. Complete information and installation instructions can be found in the “Afaria 6.0 Reference Documentation”.

Afaria Administrator tour

Begin on the VM desktop. Open the “Afaria Administrator” IE shortcut to open the Afaria Administrator application with all rights enabled. Choose the “Administrators” role link on the Servers List page to open the interface.

We recommend that you tour the complete UI, but you may want to pay particular attention to the following pages.

- Home > Server Status — Consolidates several points of interest for an Afaria administrator, including graphs of session activity and disk space use, the interface for stopping and starting the Afaria Server, and links to other key administrator functions.
- Server Configuration > Properties > Server identification — Identifies the Afaria Server by name, address, and port information. The Afaria Clients must use these identity values for communication.
- Server Configuration > Properties > License — Identifies all the licensing associated with this trial version. The trial includes 10 Client seats. Refer to [“Component and feature Client support” on page 12](#) for the table that summarizes the trial features by Client device type. Some licensed features, such as outbound notification for wireless devices, require additional environmental configuration settings that are not described in this document. Refer to the product documentation suite for additional reference resources.
- Server Configuration > Client Groups — Defines the Client groups that are part of this trial for your use. Afaria supports static and dynamic groups. Static groups contain only the Clients that you add to the group. Dynamic groups base membership on the results of a query that you define to create the group. Profiles, in turn, can be defined with an assignment attribute that will restrict the profile to run only with the Clients that have a matching group assignment. You can create custom groups according to your own definition.
- Server Configuration > Client Types — Includes the predefined, read-only Client types that Afaria supports. Some Client types include more than one subtype. You can create custom Client types based on one of the existing definitions.
- Policies and Profiles — Work profiles are the primary mechanism for managing the work performed by groups. The Afaria administrator creates work profiles as vehicles for associating work tasks with groups. Refer to the product documentation suite’s [“AfariaReferencePlatform.pdf”](#) for information regarding administration using policies and profiles interface.
- Administration > Channel Administration — Home for creating channels and publishing channels. Refer to the product documentation suite’s [“AfariaReferencePlatform.pdf”](#) for information about general channel administration and the suite’s [“AfariaReferenceComponents.pdf”](#) for information about specific channel component administration, such as for Inventory Manager or Security Manager. This trial image includes several predefined channels. Refer to [“Predefined profiles and channels” on page 17](#) for more information.
- Data Views > Clients — Displays Client-centric query results. The view returns basic Client type and connection data. Navigate the view tree to see the results for All Clients. This trial comes with the Windows test Client activity already displaying in Data Views. The Windows Client data also appears when you navigate the view tree to Client type > Windows. View the context menu that displays for Clients in the results pane.

- Data views > Inventory — Includes Client inventory data. Navigate the view tree to view all Clients per inventory category. Navigate to the Windows category to view the inventory data for this trial's test Windows Client. Open Clients in the results pane to view a Client's data. Clients must have run an inventory channel and delivered the results back to the Server in order for the view to populate with the inventory data.

Sample inventory scans

This trial includes sample inventory scan data that you can view in the Afaria Administrator user interface. The sample inventory files are located in the following VM folder:

C:\Afaria Inventory Scans

The folder contains several data files (.XML) that are specific to different Client types.

You can copy one or more of the data files into the following Afaria inventory folder:

C:\Program Files\Afaria\Data\Channel\Content\InventoryManagerChannel\Inbox

Allow Afaria a few minutes to poll the folder. The data populates the Afaria Administrator's Data Views > Inventory page when polling is complete.

Afaria trial VM Do's and Don'ts

Consider the following “Do's” and “Don'ts” as you use the Afaria trial VM.

- Do — Do adjust connection time outs if they are interfering with your actions. The Afaria Administrator web application is subject to the VM's IIS connection timeout settings. You may want to adjust the connection time out settings if you experience frequent time out messages.
- Do — Do limit the number of trial instances in your network to a single trial. You are licensed to run one trial machine.
- Do not — Do not reset the port designation for HTTP communications to the default setting, port 80. Using port 80 on the VM creates a port conflict with the host's HTTP default ports. The VM is using non-default settings for this trial.
- Do not — Do not enable SSL with default port settings. You can enable SSL if you adhere to the following guidelines:
 - Import your own SSL certificate. Refer to the documentation suite's “AfariaReferencePlatform.pdf” guide (topic “Server Configuration” > “Properties” > “Client communication”) for information about creating a SSL certificate request, generating your private key, and importing certificates.
 - Enable SSL for the XNET protocol or for HTTP on the Afaria Administrator's SSL page. Use the Enable SSL or Enable HTTPS check boxes, respectively.
 - Change the port values on the SSL page to non-default values.

Afaria features and Clients

This trial includes most Afaria features, but does have some features excluded to simplify the trial experience. The feature selections make it simpler to take a self-driven tour of the Afaria product and more suitable for trial in a VM environment.

Those seeking more Afaria features are encouraged to contact your Afaria representative to plan a full-featured trial. Find contact information in the enclosed documentation.

Component and feature Client support

Afaria support for components and features may differ across different Client types. The components and features are delivered either with the base product or through additional licensing. The following table indicates Afaria support for operating with specific Client types. Refer to each Client type's system requirement statements for detailed support information.

Table key:

X — Component or feature is supported in the complete Afaria product and in the trial virtual image.

✗ — Component or feature is supported in the complete Afaria product, but not in the trial virtual image.

<i>Afaria feature or component</i>	<i>Afaria client type</i>								
	BlackBerry	Java	Palm	Windows Mobile Professional ¹			Windows Mobile Standard ¹	Symbian	Windows
				Windows Mobile 5/6	Windows Mobile 2003	Windows CE			
OTA deployment	✗		✗	✗	✗		✗	✗	✗
Remote wipe				X	✗		X		
Byte-level differencing				X		X	X		X
Outbound notification, TCP/IP		✗		✗		✗			✗
Outbound notification, email-based SMS	✗			✗	✗		✗		✗
Device monitoring				X			X		
Client-side scheduling	X			X		X	X	X	X
Backup Manager			X	X		X	X	X	X
Access Control for Microsoft Exchange				X	✗		X		
Configuration Manager	X		X	X			X	X	
Document Manager			X	X		X			X
Inventory Manager	X		X	X	X	X	X	X	X
License Manager	X		X	X	X	X	X	X	X
Patch Manager									✗
Data Security Manager			X	X	X		X	X	X

Afaria client type (Continued)

<i>Afaria feature or component</i>	BlackBerry	Java	Palm	Windows Mobile Professional ¹			Windows Mobile Standard ¹	Symbian	Windows
				Windows Mobile 5/6	Windows Mobile 2003	Windows CE			
Session Manager	X	X	X	X	X	X	X	X	X
Software Manager			X	X	X	X	X	X	X
Remote Control				X	X		X		X
SMS Integration Suite	X		X	X	X	X	X	X	X ²

Table footnotes:

- 1 Windows Mobile Professional is an Afaria Client type that includes device subtypes. For the sake of identifying different levels of support in this table, the subtypes are listed separately.
- 2 SMS Integration Suite support for Windows requires licensing a server add-on component.

Creating, deploying, and configuring the Afaria Client



Detailed instructions for creating, deploying, and configuring the Afaria Client handheld devices are available on the Afaria news group. See [“Afaria trial news group” on page 3](#) for more information and a link to the group.

Refer to the documentation suite’s “AfariaReferencePlatform.pdf” guide (topic “Appendix A – Create Afaria Clients”) for important information about task prerequisites, creating Afaria Client software, and deploying and installing Client software on your computing devices.

Use the Create Client Installation Wizard application to create Afaria Client software. Begin on your desktop and choose Start > Programs > Afaria > Afaria Create Client Install to open the wizard. The wizard includes context-sensitive help to guide you through the process.



Every Afaria Server includes an Afaria Windows Client. You may use the Client to test operations and to manage the Server as a Client. Begin on your desktop and choose Start > Programs > Afaria > Afaria Channel Viewer to open the Afaria Channel Viewer application. Client data populates the Afaria database and displays in the Afaria Administrator interface.

Consider the following items about using this trial’s Afaria Client software:

- Predefined Clients are located on the virtual machine in “C:\Afaria Client Kits” and on the host machine’s trial extraction folder (default location C:\AfariaTrialSystem\Afaria Client Kits). If you accepted trial delivery by DVD, then an additional copy of the folder is included in the DVD root for easy transport to another computer. The desktop’s “Afaria trial VM – Start here” folder includes a shortcut to the virtual machine’s kit folder.
- Each predefined Client file in the kit folders has an associated .DOC file that summarizes the wizard settings used to build the Client.
- This trial does not include the Afaria over-the-air deployment feature. Therefore, all handheld device types require a cradled connection to install the Afaria Client. The computer hosting the Afaria Client software must be equipped with the desktop software for managing and synchronizing the handheld devices that you plan to trial. For example, you must have ActiveSync installed to install the Afaria Client on a Windows Mobile device (Professional or Standard). The host computer, in this instance, may or may not be the same computer that hosts the Afaria trial virtual machine. Use the device’s desktop software to install the Afaria Client onto the device.

Connecting Client devices to the Afaria Server



Have your Afaria Client in a cradled or wireless state when you attempt to connect to the Afaria Server, based on Client type. This trial supports the following connection methods for handheld Clients to run Afaria sessions after the Afaria Client is installed:

- Wireless¹ — BlackBerry, Symbian
- Cradled — Palm, Windows Mobile Professional, Windows Mobile Standard

1. The connecting Afaria Client must have network IP access to the Afaria virtual machine. BlackBerry and Symbian devices do not support cradled connections, so they must connect wirelessly either through carrier or WiFi. You can test connectivity by pinging the virtual machine by name or by IP address.

Launch connection

- 1 Locate the Afaria program on the device's program list after using desktop software to install the program.
- 2 Open the program and choose Connect to attempt a connection to the Afaria Server if a connection attempt does not launch automatically.
- 3 Monitor the log information that appears on the screen to view the connection status details.

All predefined Afaria Clients are seeded by default with the virtual machine name, "WIN2K3R2EE", as an address to use for connecting to the Afaria Server. However, it will be necessary to change the Client configuration from using the machine name to using the virtual machine's IP address if you experience name resolution issues when attempting to connect to the Afaria Server. Name resolution issues are observed as "Server not found" messages on the Afaria Client's user interface that occur while attempting to connect to the Server.

Change configuration from machine name to IP address

Use the following general steps to change your Afaria Client's Server address from machine name to IP address. You must know the virtual machine's IP address to complete these steps.

- 1 Open the Afaria Client program.
- 2 Open the application's menu and select the Configuration option.
- 3 Change the Server value from the virtual machine name to the virtual machine's IP address.
- 4 Save the changes and return to the Afaria Client home screen.

You can now choose **Connect** to initiate a new connection to the Afaria Server using the new setting.

Predefined profiles and channels

To give you a jump start, this trial includes several predefined profiles, channels, and channel sets. Refer to the product documentation suite's "AfariaReferenceComponents.pdf" for information about profiles and specific channel component administration, such as for Inventory Manager or Security Manager.



◆ Channels are either in a published or unpublished state. Clients can run only the published channels. A green sphere next to a channel indicates that a channel is published. You cannot edit a published channel unless you first unpublish it or create a working copy and edit the copy. Refer to the product documentation suite's "AfariaReferencePlatform.pdf" for information about editing, publishing, and general channel administration.

Case study: Acme, Inc.

The predefined channels that were created for this trial were designed to address the requirements of a fictitious company called Acme, Inc. Acme is a retailer that sells and services carpet rollers and carpet installation equipment. They have several retail locations with a growing number of frontline mobile executives, sales representatives, and field service technicians. What was once a manageable fleet of same-model laptops and cell phones, has become an unmanageable fleet of diverse computing devices. Laptops and tablets of different makes, models, and operating systems; smart phones and handheld devices from a variety of manufacturers using different operating systems and communication protocol; all operating on different regional networks and all with different user requirements.

Acme recognizes that mobile devices that carry Acme's sensitive and competitive data, along with valuable intellectual property, require a robust security solution that protects the company from loss or harm in the event of device loss, destruction, or intruder attack. Acme also recognizes that each of these computing devices is a lifeline for its frontline user that requires a complete management solution. The user could be rendered ineffective amongst customers and competitors without the business-critical information and productivity applications that give each device its purpose.


Acme's IT group is challenged with finding and implementing a secure management solution that supports frontline productivity with current data and required productivity tools. It must give frontline users the information they need, at anytime, on any device. The following table identifies their goals and requirements and the Afaria solution for each of their goals. The sample channels in this Afaria trial represent sample approaches to solving the enterprise concern.

Enterprise concern

Enterprise requirement and the Afaria solution

Security

Requirement — Keep device data and all device communications password protected and secure from unauthorized users.

 *Afaria Data Security Manager*

Set and enforce security settings, including power-on password protection and data encryption. Controls for password protection include password composition and the number of password attempts before lock down. Controls for handheld Client data encryption include allowing selective encryption of PIM databases, files, and removable card data. Data encryption for Windows Clients includes drives and removable media. Afaria Administrator includes a recover password feature to allow Data Security Manager Client users to recover password access to their Client after having forgotten their password.

Data Security Manager channels for handheld Clients in this trial include administrator passwords that are set to a value of "1234".

Device configuration

Requirement — Establish and maintain a base device configuration policy that can replace the need to have each device handled by the IT staff before deployment to its user and establish some consistency across devices. The policy is likely to vary based on each device's features and capabilities and the user's region and role.

 *Afaria Configuration Manager*

Remotely configure and maintain devices that are deployed to your mobile workforce. You can create channels to specify particular attributes, preferences, and settings on these devices, which allows your Client users to spend less time configuring and managing their devices and more time meeting business objectives.


Configuration Manager channels in this trial include some very basic and arbitrary settings. You can edit the channels to apply settings that are of interest to your enterprise.

Enterprise concern

Enterprise requirement and the Afaria solution

Inventory asset tracking

Requirement — Track and maintain information about each computing device. The information must include enough detail about a device's hardware and software attributes that IT can perform a meaningful analysis of its device fleet.

 *Afaria Inventory Manager*

Centralize the monitoring and reporting of hardware and software resources installed on your Clients. Inventory Manager silently detects installed hardware and software on the Client during the communications session or while the Client is disconnected. Use a subsequent communication session to transfer results to your database. Streamlined inventory data reporting is accomplished by transmitting only data that has changed since the last inventory scan. Other corporate asset tracking, accounting, and help desk systems can access the data from the database.


Inventory Manager channels in this trial scan hardware and software data from Clients. Inventory Manager processing subsequently reports the data back to the Afaria Server for retention in the Afaria database. You can review inventory data in the Afaria Administrator's Data Views for inventory or Clients, or in the inventory report. Some of the channels are associated with a daily schedule.

The two Inventory Manager channels in the Win32 Channels folder differ in that one of the two channels is associated with a daily schedule and has autosubscribe enabled. The autosubscribe attribute makes the channel mandatory for the Client and the daily schedule makes it run without user interaction. The other channel will be visible to the Afaria Client user, but optional.

Refer to "[Sample inventory scans](#)" on page 9 to learn how to add sample inventory data to the Afaria Administrator's Data Views > Inventory page.


File management

Requirement — Keep shared documents synchronized between frontline users and the enterprise. The enterprise and the end users must stay current with the documents that are new, have changed, or have become obsolete.

 *Afaria Document Manager*

Publish groups of documents for Client users to access. Document Manager channels can include text files, bitmaps, HTML files, and more. You can define Document Manager channels to “push” content to connected Client users, or you can allow users to decide whether they want to subscribe.

Document Manager channels in this trial include a setting to allow Client channel subscribers to pick Document Manager files individually.


 *Afaria Session Manager*

Session Manager channels are created by scripting worklists or sendlists to meet your specific needs. You can automate electronic file distribution, file and directory management, notifications, and system registry management tasks. Worklists and sendlists are the units of activity for all work on and between the Server and Clients.

The Session Manager channel in the Win32 Channels folder performs some file synchronization functions. This channel will not be effective in its current state unless you create a folder structure on both the Afaria Server and the Afaria Client that matches the folder structure used in the channel’s worklist of events.

Backup and restoration

Requirement — Perform routine backups for application data and documents. Backup content must be recoverable in the event of loss or destruction.

 *Afaria Backup Manager*

Back up and restore large quantities of data from specified files, folders, and applications to a specific folder structure on the corporate network. For handheld Clients, applications and data missed by PIM sync processes are backed up and can be restored when these Clients connect to the Server.

The Backup Manager channels in this trial will not be effective in their current state unless you have a matching folder structure on the Afaria Client that matches the folder structure used in the channel’s backup item definition.

Enterprise concern

Enterprise requirement and the Afaria solution


Software distribution Requirement — Distribute and install or upgrade enterprise software applications. Software applications may be commercial or custom.

 *Afaria Software Manager*

Distribute and install commercial or custom-built software applications on Afaria Clients. You can push software packages to your Clients after they initiate a connection to ensure that users have the latest software, or you can let Client users subscribe to channels so that they install only the software they need.

The Software Manager channels in this trial is designed to deliver a software setup package to the Afaria Client for installation. You can also plan to deploy the package from a single LAN connection, rather than deploying the package to each Client.

Policy enforcement Requirement — Enforce the Acme policy that prohibits using company resources for personal use. Specifically, IT maintains a list of blacklisted software applications that it scans for on the LAN. IT must be able to detect prohibited applications on its mobile devices.

 *Afaria Session Manager*

Session Manager channels are created by scripting worklists or sendlists to meet your specific needs. You can automate electronic file distribution, file and directory management, notifications, and system registry management tasks. Worklists and sendlists are the units of activity for all work on and between the Server and Clients.

The Session Manager channel in this trial called “Blacklisted Application Check” checks for applications that are in violation of enterprise policies. It uses a worklist that is written with a variety of events. The worklist logic is defined as follows:

- Use a LOAD SCRIPT event to load a VB script that contains XML file parsing logic.
- Load an XML file (C:\vbscripts\prohibited.xml) to identify the list of blacklisted applications. You can edit this file to add some of your own sample applications to the list.
- Use nested IF events to establish variables for Client paths based on Client type.
- Use a REPEAT WHILE event, RUN SCRIPT FUNCTION event, and nested IF events to iterate through the XML list while searching the Client for a matching application and sending messages to the Client interface. Instances of finding a blacklisted application raise an event in the Afaria Administrator interface. The administrator can visit the Home > Server Status page or Home > Alerts page to receive event notifications.

