SYBASE®

Installing Afaria® 6.5

Afaria helps you manage all the pieces of your mobile infrastructure, including desktop and laptop computers, and your mobile devices. From a central location, you can keep devices secure, deploy applications, check inventory and provide automatic updates to your frontline workers.

This guide provides overviews and step-by-step information about how to install, configure, and begin using the Afaria Server, Afaria Administrator and related applications.

Installing Afaria 6.5

Document version 6.50.00

Contents

Preface

This guide is for the person responsible for installing and maintaining the Afaria Server and Afaria Administrator programs. We recommend that you have a working knowledge of the Windows operating system and its conventions, your database server, IIS, Microsoft Internet Explorer and a directory manager such as LDAP. You also need a working knowledge of the device types you plan to support.

Afaria SMS Integration Suite customers should start the Afaria setup program, choose the **Documentation** option, and then navigate the documentation folder and use document *Installing Afaria SMS Integration Suite* for installation guidance and instructions.

Finding User Assistance

Afaria provides documents and support for Afaria operations.

Afaria Documentation

The following documents are available with the product image in the \Documents directory. All documents are in PDF format.

- *Getting to Know Afaria* – Presents an overview of the Afaria product and how it can help you provide valuable tools and security for your enterprise.
- *Installing Afaria* – Explains how to install and configure the Afaria server. Afaria SMS Integration Suite customers should refer to *Installing Afaria SMS Integration Suite.*
- *Installing Afaria SMS Integration Suite* – Explains how to install and configure the Afaria SMS Integration Suite product. This document is only for Afaria SMS Integration Suite customers.
- *Afaria Reference Manual* | *Platform, Afaria Reference Manual* | *Components* – Provides conceptual and detailed information about the Afaria product and its key features.These guides are also available from the user interface.
- *Afaria Reference Manual* | *APIs* – Contains all server and client APIs for developing custom applications to interface with your Afaria solution.

Afaria Support Services

Product technical support: www.sybase.com/support or frontline.sybase.com/support

Americas and Asia-Pacific call support:

Email – afariasupport@sybase.com

(678) 585-7320 Atlanta, Georgia

(800) 669-1211 Toll-free

European call support:

Email – emea-afariasupport@sybase.com

+44 (0) 1628 50 5321 United Kingdom

0825 800372 Toll-free

About Afaria Architecture

The Afaria architecture is designed for your enterprise environment to help you manage your desktop and mobile computing devices.

The following Afaria terms help to provide an understanding of the Afaria solution:

- Server – Afaria is a server-based solution that supports a single server or server farm environment. The server communicates with the Afaria database, the Afaria Administrator, the Afaria Over-the-Air (OTA) Deployment Center, the relay server, and Afaria clients. It is the central point for all Afaria activity.
- Afaria Administrator – Afaria Administrator is the Web application that provides an interface for the Afaria server. You use Afaria Administrator to define the server configuration, define access policies for Afaria Administrator users, create and manage Afaria clients, monitor system activity, and communicate with other Afaria servers.
- Afaria clients – Afaria clients are user devices, such as laptops, handhelds, and phones that run Afaria Client software. Clients initiate connections with an Afaria server to run sessions. Servers use sessions to manage the clients, deliver client updates, and to collect data from the client. Depending upon your licensing, several client types are available, so you can choose which one best suits your users' needs.
- (Optional) OMA DM server – The OMA DM server runs authenticated sessions with OMA DM clients to deliver messages that manage OMA DM clients. Clients are devices that have native support for device management via OMA DM standards and are known to the Afaria server.
- (Optional) Relay server – The relay server operates as a proxy for HTTP and HTTPS sessions between the Afaria server and its Afaria clients. The relay server enables you to further secure your enterprise network by moving the session connection point from within your firewall to a location outside of your firewall, to your Demilitarized Zone (DMZ).
- (Optional) OTA Deployment Center – A Web server that you install to provide software deployment services for your clients. An administrator pushes Afaria client installation packages out to the deployment center and then sends notices to device holders. Device holders can download the client directly onto their device for installation.

About Afaria Server

The Afaria Server program has no user interface. This is also the server that communicates with the database. Depending upon your licensing, other Afaria programs that reside on the Afaria server include:

- Create Client Installation – The Create Client Installation program is a wizard that guides you through creating a client installation package. Based on client type, you can choose different options that allow you to deploy the client via the OTA Deployment Center, a companion PC, a network, or client APIs.

- Software Catalog Editor – The Afaria Inventory Manager component references a software catalog when reporting software installed on clients. It can detect and report all software defined in the software catalog, which includes a listing of most commercially available applications.
- Channel Viewer – Requires a Windows client license. Channel Viewer lets you run Afaria sessions directly on your server machine.
- OTA Publisher – This utility lets you create and publish "packages" of client setup files to a Web server deployment center (Afaria OTA Deployment Center) for deployment to your planned client devices. A device user can download a package from the deployment center to install the Afaria client on his device without having to connect to a companion PC or network.

About Afaria Server Farms

A server farm is a group of servers acting as a single entity. Afaria server farms support the shared use of a centralized Afaria database, which contains information about logging, inventory, and alerts. Data is accessible by all members of the farm. A dynamically elected machine in the farm runs the alerts rules engine and the alerts notification, as well as change detection for the entire farm. The *Afaria Reference Manual* | *Platform* contains more information on configuring and responding to alerts in a farm environment.

The main Afaria server is the source for creating and managing all clients. The database is shared with all servers in the farm and read-only versions of specific information is replicated from the main server to the remaining servers. Clients can connect to any server in the farm. This architecture provides a scalable, load-balanced solution when you have many clients connecting simultaneously.

About Afaria Administrator

Afaria Administrator is the Afaria Server program's "interface," a Web-based program that you can access from any computer running appropriate versions of Microsoft .NET and Internet Explorer. Afaria uses role-based access policies to control user rights. Rights are associated with discrete functions in the user interface. An administrator with sufficient access policy rights can use Afaria Administrator to view and manage operations and data. A user with limited rights might be limited to view-only access of a single functional area.

System Requirements and Release Notes

Before you install your Afaria components, validate all the prerequisites and system requirements in order to take full advantage of its features and to ensure that the your system operates with maximum efficiency.

- Complete system requirements are available in the product release notes available on the technical support site. You must ensure that your environment complies with the system requirements before installing Afaria.
- Running Afaria and RemoteWare® products on the same machine is not supported; you must install each product on a separate machine.
- Installing Afaria and its associated server-side components requires that you have physical access to the target servers. Using terminal services or comparable means is not a viable method for installation.

Preparing to Install Afaria

Before you install your Afaria components, take steps to prepare your environment.

Configuring Your Database

The Afaria server uses a database to log all system activity, such as inventory data, file transfers, and alerts. You must install and configure your database prior to installing the Afaria Server program. If you are planning to create a server farm environment, select the database only when you install the main server; all the servers in the farm access the same database.

The product supports using Microsoft SQL Server, Oracle, or iAnywhere SQL Anywhere for the Afaria database. Configure only one type of database.

Refer to the system requirements for complete database support information. System requirements are available in the product release notes on the technical support site or from your Afaria representative.

Determining Your Database Size

All logging was enabled for tests determining growth rate of database.

You can use the following formula to estimate database disk space growth per day:

(# of Sessions per day) * (average session size) = Estimated growth per day

For example, to determine the weekly disk space growth for 1000 daily sessions with an average session size of 60 KB:

(1000 sessions per day) * (60 KB average session size) * 7 days = 420 MB

So in this example, the database is estimated to grow by 420 MB per week.

Also note the following:

- You should add 1 MB of data to our estimate for each Inventory Manager client. Using Inventory Manager to perform client directory scans on Windows clients adds significantly more data to this estimate.
- Sessions with 100 events add an average of 40 KB in database growth per session in additional log data.

Setting Up SQL Anywhere for Afaria

Complete the following tasks to create and connect to your database if you plan to use SQL Anywhere database with your Afaria product.

1. Create a database. Use default configuration settings with the exception of the following attributes:
   - Install jConnect metadata support – Disabled.
   - Page size – 8192 KB minimum.
2. Create a database user for the Afaria service to use for database access. You must assign the database administrator (DBA) authority to the user.
3. Connect to the new database using the following network database server properties:
   - Identification – Database user name and password that you created for Afaria database access.
   - Database – Indicate the Afaria database server name and start line "dbsrv11.exe", as well as the database name and file.

Do not start the database using start line "dbeng11.exe", which is for non-network database servers and does not support enough database connections for the Afaria service.

It is strongly recommended that you have only one instance of dbsrv11.exe per database.

For ongoing operations, prepare your SQL Anywhere environment for sustainability and availability.

1. Create a Windows service to automatically start your database when the server restarts. Using the Sybase Central folder view (**View** > **Folders**), select SQL Anywhere, click the **Services** tab, and launch the new service wizard.
2. Create an event to backup and truncate the log. We recommend a log size of 50 MB.

   For more details about using the new service wizard or configuring the SQL Anywhere database and using a system event to trigger log truncation, see your SQL Anywhere documentation.

Setting Up SQL Server for Afaria

Complete the following tasks to configure your Microsoft SQL Server database for Afaria.

1. Create a database with the following attributes:

   Datafiles – Select **Automatically Grow File** and **Unrestricted filegrowth**.

   Transaction Log – Set the size to a minimum of 25 MB. Select **Automatically Grow File** and **Unrestricted filegrowth**.
2. Create a new Administrative Login for Afaria and use the following stored procedure to give the user database rights: **sp_addalias '*account name*', 'dbo'** and run this command against your Afaria database.

3 Verify that Afaria logs are truncated on checkpoint. You must complete the following steps to truncate the logs:

   1 Right-click the database and select **Properties** on the shortcut menu.
   2 In the Properties window, click the **Options** tab.
   3 In the Recovery section, select **Simple** from the **Model** drop-down list box.

You can also use the Windows Authentication option by aliasing your Windows login as a DBO. For more details, see your Microsoft SQL Server documentation.

Setting Up Oracle for Afaria

Complete the following tasks to configure your Oracle database for Afaria.

1 Install the Oracle client on the planned Afaria server.

2 Create a user account on the Oracle Server. Grant the account the following roles and system privileges to the database:

   - Role – Connect, Resource
   - System Privileges – Create Table, Create Trigger, Create View, Create Sequence, Create Procedure, Unlimited Tablespace.

3 Create a Net service to allow the planned Afaria server to communicate with the Oracle Server.

4 Restart the Afaria server.

For more details on configuring the Oracle database, see your Oracle documentation.

User Accounts for Installing and Operating Afaria

Afaria runs as a Windows Service, which means the server operates without an administrator logging on to start the program. If the server reboots, Afaria starts automatically.

Afaria installation and operations require a user account that is either a local account that is a member of the Administrators group, or a domain account that is a member of the local administrators group.

The account must have the following attributes:

- Password Never Expires
- Logon as Service

  When you install Afaria, you'll enter this user account and its password. This local account must exist with the same password in each of the domains you plan to authenticate against for Afaria operations.

Preparing the Platform for Upgrade

You can upgrade to Afaria 6.5 from any 5.5 SP2 or 6.0 configuration. Afaria 5.5 customers must apply 5.5 SP2 to the Afaria server before upgrading to Afaria 6.5. Afaria 5.5 SP2 clients can then upgrade directly to Afaria 6.5.

Before you upgrade your Afaria components, validate all the prerequisites and system requirements in order to take full advantage of its features and to ensure that the your system operates with maximum efficiency.

- All customers are advised to have an Afaria system backup in place prior to beginning an in-place upgrade. A system backup includes the database, application software, and application data.
- Complete system requirements are available in the product release notes available on the technical support site. You must ensure that your environment complies with the system requirements before installing Afaria.

Afaria Server Upgrade

The following steps summarize the procedure for upgrading an Afaria server installation that includes a single Afaria server.

1. Stop Afaria services.
2. Upgrade the server. Do not start the Afaria service at this time.
3. Start Afaria Server services.

Afaria Server Farm Upgrade

Upgrading a farm environment has additional requirements to complete the upgrade. The following steps summarize the procedure for upgrading an Afaria server farm environment.

1. Stop Afaria services on all replication servers.
2. Upgrade the main Afaria server. Do not start the Afaria service at this time.
3. Upgrade the replication servers.
4. Start Afaria Server services on main and replication servers.
5. Replicate appropriate channels to replication servers.

Preparing for Continued SSL Communications

For environments that operate with SSL communications, continuing SSL support may be critical to your operations. Consider these items to ensure that your SSL sessions can continue without interruption:

- Valid certificate requirements – Afaria 6.5 allows SSL sessions to run only when the server's certificate is valid, as evaluated against the following criteria:
  - The certificate is signed by a trusted CA or a trusted self-signed CA.
  - The certificate is not expired.
  - The Common Name—typically the fully qualified domain name—on the certificate matches the address that the client used to initiate the session.
  - The certificate is valid for encryption and authentication.
  - The certificate is compliant with x.509 certificate standards. Supported formats: Base64-encoded x.509 (.CER) and Personal Information Exchange (.PFX).

    You can convert a nonencoded x.509 certificate to a Base64-encoded certificate by using a "save as" or export process in a certificate editor such as the Microsoft Certificates utility (CertMgr.msc).

    If the product detects an invalid certificate after the upgrade, all SSL connections are terminated until a new, valid certificate is installed.
  - The certificate key is an RSA key.
- Certificate password assignment – In contrast to previous releases, the upgraded environment requires a password for all certificates. Therefore, to facilitate a working environment after upgrade, the upgrade assigns password "password" to the certificate. You can use the **Server Configuration** > **Properties** > **Client Communication** > **View** to view your certificate and change the password to a privately known value.

Preparing for Continued OMA DM Operations

For customers upgrading from Afaria 6.0 FP1 or FP3 and currently using the OMA DM trust task, you must replace the task to adopt new implementation. These steps outline the replacement procedure within the context of the upgrade:

1. Upgrade server and administrator.
2. Restart services.
3. Modify existing trust task, change action to remove.
4. Add a new trust task into the same policy but after the pre-existing trust task. Define the task with an add action and select any additional rights to enforce.
5. Connect OMA DM clients to deploy updated policy.

Preparing for the Multitenancy Environment

Multitenancy is a separately licensed product feature that allows hosting providers to manage multiple enterprises from a single Afaria implementation.

See also *Afaria Reference Manual* | *Platform* > “Using Tenants and Multitenancy” to learn about multitenancy and how it supports your role as a hosting administrator.

Transitioning Clients and Assets

A newly upgraded environment, one that has been upgraded from a nontenant environment to a multitenant environment, continues operations without disruption to scheduled client sessions or the work tasks operating in the pre-upgrade environment. All upgraded clients and assets, such as profiles and their associated policies and channels, default to the predefined system tenant during the upgrade.

After upgrading, follow this general workflow to migrate your client base from single-tenant operations to multiple-tenant operations without interrupting schedules or work:

1. Define tenants.
2. Define access policies that associate roles with tenants.
3. For each tenant, define assets and connect clients:
   - Define client groups.
   - Define profiles and associated assets that continue your operations according to your requirements.

     You may continue to use system tenant assets, as shared by the system tenant and available to all tenants, or you can define new, tenant-specific assets.
   - Assign client groups to profiles, as appropriate for your operations.
   - Change client tenant associations from the system tenant to the new tenants.
   - Connect clients.

   When clients connect, they automatically pick up their new tenant association and begin using their assigned profiles.

New Access Policies Tenant Role Definition

A new Afaria Administrator Server Configuration Tenants page introduced by the multitenancy feature introduces a new Tenant role definition item in the Server Configuration role definition tree. The Tenant role definition attribute defines the user rights for the new page as read only, modify, or create. Revisit access policy roles after the upgrade to determine whether the postupgrade value for the Tenant attribute is appropriate for your requirements.

Upgrading Custom Data Views and Custom Reports

Database changes introduced by the multitenancy feature have implications for custom data views and custom reports. The upgraded environment attempts to filter results by tenant by modifying the associated SQL script at runtime. However, these modifications may not always be successful. Therefore, revisit your custom items after performing the upgrade, creating a few tenants, and accumulating some data in each tenant to evaluate how the item is performing and understand whether the data returned is filtered by tenant. Custom items produce one of the following results:

- Error-free results that are filtered by tenant
- Error-free results that are not filtered by tenant
- Fatal errors during execution

  You may need to delete damaged items and re-create them in the new environment, taking the new database design into consideration.

Additionally, custom items that you create after the upgrade are available to all tenants, rather than only for the originating tenant.

See also *Afaria Reference Manual* | *Platform* > “Data Views” to learn more about creating custom views in a multitenant environment.

Preparing the Clients for Upgrade

Afaria client upgrades occur automatically, using the Afaria Electronic Software Delivery (ESD) feature, as your clients connect to an upgraded Afaria server. When upgrades fail due to the Afaria platform no longer supporting a client's operating system, the system records the event in the Messages log.

The upgrade connection performs only an upgrade and does not execute other operations, such as running requested channels. Use a subsequent connection to continue operations.

Upgrading Data Security Manager Clients that Use Encryption

Data Security Manager method for interpreting paths and file names for encrypting and specifying items is changed. In summary:

A folder name now requires a backslash terminator. Folder names without a backslash is interpreted as a file. For example: \Temp\ declares a folder, while \Temp declares a file. This distinction may render previously encrypted files as decrypted. Consider the following cases:

- Pre-upgrade specification: \Temp
  - if \Temp directory exists, all files in directory are encrypted.
  - if \Temp directory does not exist but file "temp" does, encrypt only the file
- Upgrade specification: \Temp encrypts only file "temp" without regard to presence or absence of directory of same name
- Upgrade specification: \Temp\ encrypts all files in folder

See also *Afaria Reference Manual* | *Components* > Data Security Manager for Handheld Clients > Lock Down Options > "Path and File Name Data Items" to learn defining items for encryption and items for deleting specified data.

Upgrading Clients for the Multitenancy Environment

See "Preparing for the Multitenancy Environment" on page 16.

Preparing the Pre-6.0 Platform for Upgrade

You can upgrade to Afaria 6.5 from any 5.5 SP2 configuration. However, customers who have already upgraded to Afaria 6.0 have already migrated into a newer Afaria environment that includes significant infrastructure changes from pre-6.0 versions. As a customer upgrading from a pre-6.0 version, you have additional preparation. This topic and its related subtopics all describe additional information for your upgrade path.

Before you upgrade your Afaria components, validate all the prerequisites and system requirements in order to take full advantage of its features and to ensure that the your system operates with maximum efficiency.

- Afaria's version 6.0 introduced significant changes for managing your Afaria clients. The nature of the changes represents a new paradigm for managing clients. Rather than using a channel-centric approach to manage clients, work profiles are now used to manage clients. It is critical that you learn about the upgrade process in advance of executing the upgrade to avoid unexpected results. See "About the Profile Platform" on page 21.
- All customers are advised to have an Afaria system backup in place prior to beginning an in-place upgrade. A system backup includes the database, application software, and application data.
- Complete system requirements are available in the product release notes available on the technical support site. You must ensure that your environment complies with the system requirements before installing Afaria.

Afaria Server upgrade

The following steps summarize the procedure for upgrading an Afaria server installation that includes a single Afaria server.

1. Evaluate your channels, channel assignments, and client-side schedules in preparation for post-upgrade management. See "Evaluating Your Current Environment" on page 30.
2. Stop Afaria services.
3. Upgrade the server. Do not start the Afaria service at this time.
4. Review your upgrade exception report to evaluate and resolve exceptions. See "Reviewing Your Reports After Migration" on page 33.
5. Start Afaria Server services.

Afaria Server farm upgrade

Upgrading a farm environment has additional requirements to complete the upgrade. The following steps summarize the procedure for upgrading an Afaria Server farm environment.

1. Evaluate your channels, channel assignments, and client-side schedules in preparation for post-upgrade management. See "Evaluating Your Current Environment" on page 30.
2. Stop Afaria services on all replication servers.
3. Upgrade the main Afaria server. Do not start the Afaria service at this time.
4. Upgrade the replication servers.
5. Review your upgrade exception report to evaluate and resolve exceptions. See "Reviewing Your Reports After Migration" on page 33.
6. Start Afaria server services on main and replication servers.
7. Replicate appropriate channels to replication servers.

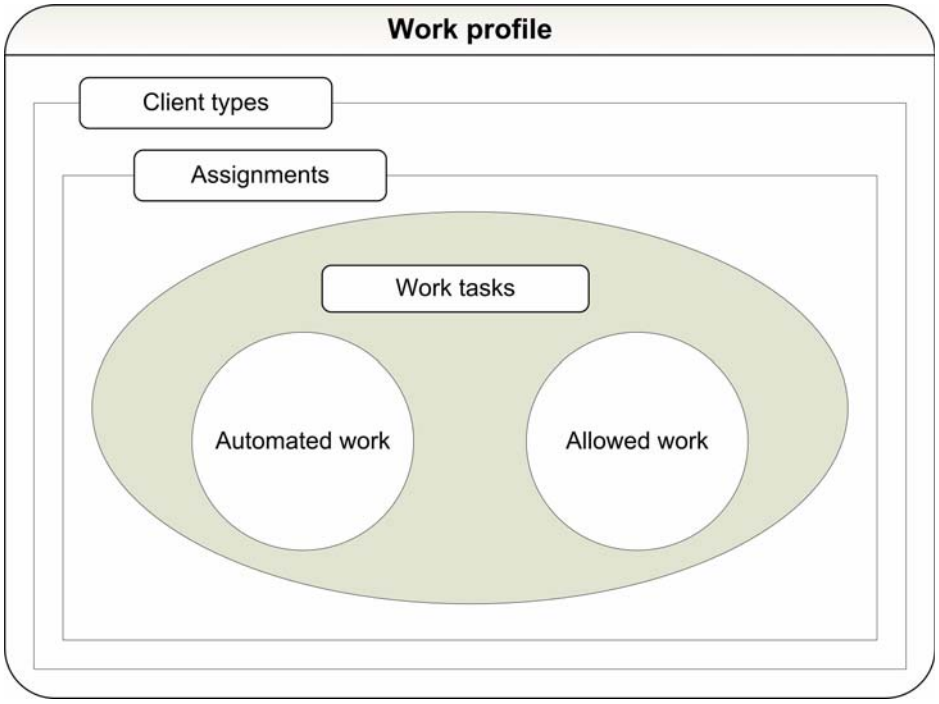
About the Profile Platform

- It is critical that you learn about the upgrade process in advance of executing the upgrade to avoid unexpected results.
- For Afaria installations that cannot tolerate the downtime that may be associated with procedures necessary to upgrade and adjust your environment to the new implementation, you are strongly advised to consider engaging Sybase Professional Services for consulting and operational assistance.

- It is recommended that you consider different upgrade strategies before beginning your upgrade. See "Upgrade Strategy: In-Place Upgrade" on page 26 and "Upgrade Strategy: New Install" on page 27.

Afaria's version 6.0 introduced significant changes for managing your Afaria clients. The nature of the change is a new paradigm for managing groups. This represents movement away from using a channel-centric approach to management to a work-profile-centric approach to management.

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. Work profiles in Afaria are primarily defined by their client types, assignments, automated work, and allowed work.



The release includes an expanded feature set for the work profiles implementation. This expanded implementation includes work profiles supporting all client types. A work profile includes tasks and allowed channels and group assignments to define automated work and allowed work. Tasks can be defined as one or more monitor-action pairs (formerly referred to as trigger-action pairs). Running a channel is a valid action in a monitor-action pair. You can use one or more profiles per group.

The paradigm shift is summarized by the following implementation changes:

- Work profiles are supported for all client types.
- Work profiles now include a client type[1] association. You can associate one or more client types to a work profile.
- Group assignments are now associated with work profiles, rather than with channels. This enables you to use a single work profile to manage work for multiple groups. You can also use a system group “All Clients” as a simple way to assign all of your clients to the work profile. The Afaria server does not send a work profile to any group until it is assigned.
- Channels no longer include schedules. This functionality is replaced by two new types of monitors (formerly referred to as triggers) that can each be included in a profile:
  - Schedule monitor – Client-side schedule functionality for one-time, daily, weekly, and monthly schedules is replaced by a new schedule monitor. Like any monitor type, you can define as many schedule monitors as you want.
  - Connection monitor – Client-side online schedule functionality is replaced by a new connection monitor. This monitor looks for the availability of a specific network connection or any connection, according to the monitor definition.
- Work profiles now include an allowed channels list. That is, a list of channels that you want to allow the assigned groups to run.
  - The practice of assigning channels without a schedule to allow clients to manually request channels is replaced by adding channels to the allowed channels list. Clients manually request channels by any available method such as using a channel parameter file (.XEC), client API call, Windows Channel Viewer, or the handheld client’s Afaria UI. Clients requesting the channel may run any channel on the allowed channels list.
  - The practice of associating a schedule with a channel to automate work is replaced by associating a schedule monitor with a run channel action. The resulting monitor-action pair is part of a work profile and the channel becomes a member on the allowed channels list. When the schedule invokes the run channel action, the client connects and requests the channel.
- Work profiles now include an optional default channel association. This enables you to associate a default action—run a channel or channel set—for any work profile. A connecting

1. A client type may include more than one sub-type. For example, the Windows Mobile Professional type includes multiple sub-types such as Pocket PC and Windows CE devices.

client runs the default channel only when the client's Afaria configuration settings do not specify a channel to run and the connection is not driven by a monitor-action pair event.

The default channel may be most frequently used when a client installation package is created without specifying a channel to run during connection. The default channel would then be used to determine the channel to run during the connection.

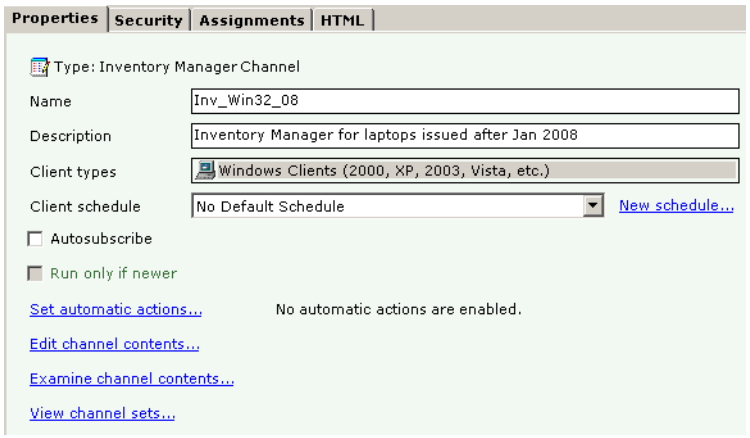
- Work profiles now include a priority value. This enables you to establish prioritization for Afaria to use to resolve conflicts for the default channel assignment when a client is assigned to more than one profile and the client's Afaria configuration settings do not specify a channel to run.
- Client-side schedules are removed from the Afaria Administrator user interface, both from the server configuration schedule page and from the channel administration page. All applications for client-side schedules are absorbed by schedule and connection monitors.
- An export/import feature is added to the policies and profiles user interface. While work profiles are stored in the Afaria database and available to all Afaria servers in a farm, you may want to use the export/import feature to copy one server's work profiles to a separate, peer server.

In order to ensure as smooth an upgrade as possible, several of the paradigm implementation changes warrant some pre-upgrade evaluation. The evaluation results may suggest that making changes prior to the upgrade improves the upgrade results.

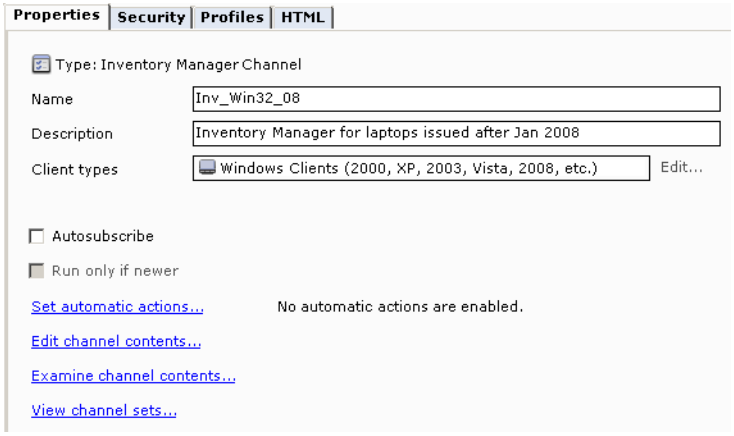
User interface differences

The following images compare the channel user interface before the upgrade to Afaria 6.0 and after the upgrade to Afaria 6.0.

Before upgrade: **Channels** > **Administration**

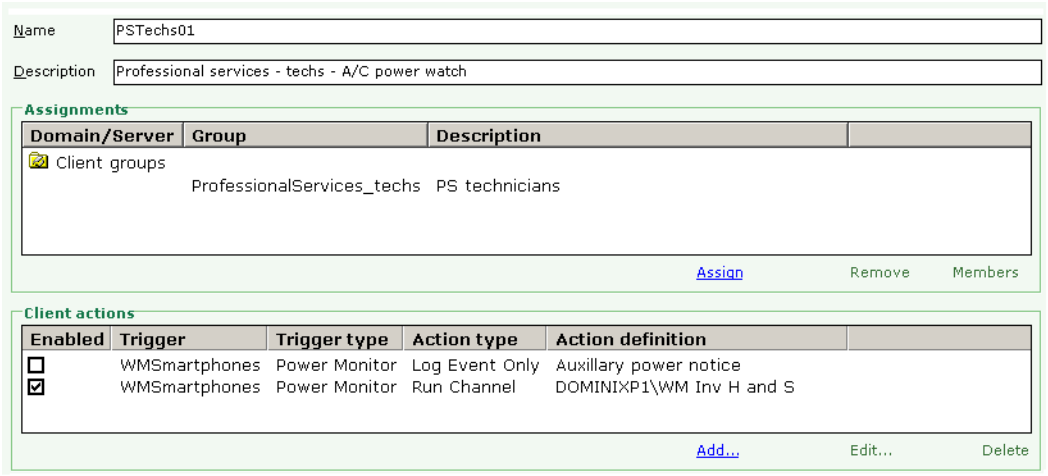


After upgrade: **Administration** > **Channel administration**

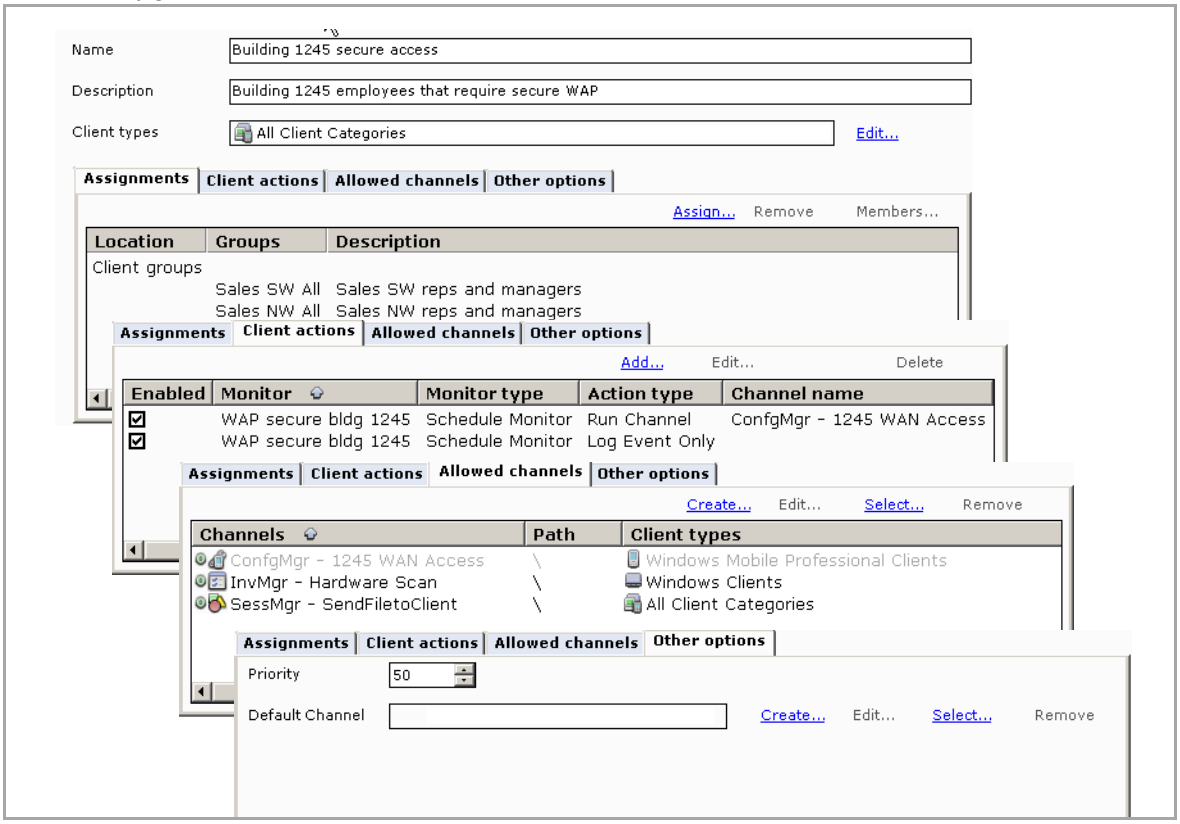


The following images compare the work profile user interface before the upgrade to Afaria 6.0 and after the upgrade to Afaria 6.0.

Before upgrade: **Server configuration** > **Policies and Profiles**



After upgrade: **Administration** > **Policies and Profiles**



Upgrade Strategy: In-Place Upgrade

An in-place upgrade is one option for upgrading your Afaria release. An in-place upgrade is performed on your production environment. It may cause an operational slowdown while you stop services, perform the upgrade, and adjust your environment to the new implementation.

You may want to consider creating a test environment to execute the in-place upgrade procedure and to evaluate the results while your production environment continues to operate.

In-place upgrade summary:

1. Evaluate your production environment. Clean up and change your implementation as needed to improve your post-upgrade experience:
   - Client-side schedules – "Evaluating Client-Side Schedules" on page 30
   - Channels and channel sets – "Evaluating Channels and Channel Sets" on page 31
   - Channel assignments – "Evaluating Channel Assignments" on page 31
2. Use the upgrade migration utility to evaluate "What if…?" scenarios for performing the upgrade. Refer to "The Upgrade's Migration Activity" on page 29 to learn about the utility.

   Performing this step provides an opportunity for you to evaluate the upgrade before executing a live upgrade.
3. Perform upgrade.
4. Review your upgrade results. Refer to "Reviewing Your Reports After Migration" on page 33.
5. Test client connections.

Upgrade Strategy: New Install

A new install is one option for upgrading your Afaria release. The strategy uses a separate hardware environment while your production environment continues to operate. When the upgrade is complete, you have established new data as needed and are satisfied with the results, you then redirect all Afaria connections to the new environment.

New install upgrade summary:

1. Evaluate your production environment. Clean up and change your implementation as needed to improve your post-upgrade experience:
   - Client-side schedules – "Evaluating Client-Side Schedules" on page 30
   - Channels and channel sets – "Evaluating Channels and Channel Sets" on page 31
   - Channel assignments – "Evaluating Channel Assignments" on page 31
2. Establish a separate, new hardware environment.
3. On the new environment, install the same Afaria version as your production environment.
4. Use export/import, peer-to-peer replication, or manual steps to duplicate in the new environment any data from the production environment that you want to continue to use after the upgrade.
5. Use the upgrade migration utility to evaluate "What if…?" scenarios for performing the upgrade. Refer to "The Upgrade's Migration Activity" on page 29 to learn about the utility.

   Performing this step provides an opportunity for you to evaluate the upgrade before executing a live upgrade.
6. Perform upgrade.
7. Review your upgrade results. Refer to "Reviewing Your Reports After Migration" on page 33.
8. Establish new data in your new environment that supports your planned client connections:
   - Work profiles
   - Schedule monitors and connection monitors
   - Client groups
   - Channels
   - Channel sets

   Use product documentation as a reference for working with new or changed features.
9. Run test sessions in new environment.
10. Redirect all clients to the new environment.
11. Retire the former environment.

Consider the following items concerning offline upgrades:

- Provides an opportunity to upgrade your server hardware.

- Minimizes production environment downtime.
- Session history and client data from your original production environment is preserved for as long as you want to store the data but is not available from within the new environment.

The Upgrade's Migration Activity

The setup program evaluates your current environment's data and migrates them to the new policy and profile implementation. Your pre-upgrade client-side schedules, channel assignments, client schedules, and so on, under the former channel-centric paradigm become schedule monitors, connection monitors, monitor-action pairs, work profile assignments, and so on, within the new work profile paradigm.

The migration upgrade creates one new work profile for each unique group assignment/client type[1] combination in your system.

The upgrade produces migration reports when the upgrade completes. Refer to "Reviewing Your Reports After Migration" on page 33 for information about the reports.

The result of an upgrade is that a client that connects after the upgrade is subject to the same client/user validation as before the upgrade, and continues to run the same channels as before the upgrade with the same schedules.

Evaluating "What if...?" Before You Upgrade

The Afaria upgrade includes a migration utility that enables you to evaluate the results that the upgrade will produce without actually performing the upgrade or making any changes on your system. Use the utility to preview the new work profiles that the upgrade creates based on the current state of your Afaria operations.

Locate the utility on the Afaria product image:

<*Root*>\UpgradePreview\UpgradePreview55.exe

Copy the utility file onto your Afaria installation and run it.

<*InstallDir*>\Bin\

The utility produces the same migration reports as when an actual upgrade completes. Refer to "Reviewing Your Reports After Migration" on page 33 for information about the reports.

1. A client type may include more than one sub-type. For example, the Windows Mobile Professional type includes multiple sub-types such as Pocket PC and Windows CE devices.

Evaluating Your Current Environment

Consider taking action prior to your upgrade to facilitate better upgrade results.

Evaluating Client-Side Schedules

Consider taking the following actions to improve your post-upgrade experience:

- Delete schedules that are obsolete for your operations – The upgrade process converts all client-side schedules into either schedule monitors or connection monitors. Obsolete schedules, such as expired schedules that you do not plan to reuse, become monitor clutter in the upgraded environment.
- Schedules with network access parameters, schedule not associated with a channel – The upgrade process drops any network access parameters that you've defined for a schedule when the schedule is not associated with a channel. However, the change is noted in a resulting exceptions report. You may update the channel to omit the parameters or allow them to drop during the upgrade. In the upgraded system, you may redefine the parameters using a new "Criteria" property when you define a monitor-action pair in the upgrade system.
- Evaluate schedules to ensure that functionality can migrate successfully – The upgrade process attempts to convert all daily, weekly, and monthly schedules to retain their defined functionality. However, the conversion may find exceptions as some schedule features were removed or changed to improve usability design.

  The upgraded environment does not support the following features for the indicated schedule types:

  - Daily schedules – Cycle attribute value greater than one when fewer than all of the days of the week selected.
  - Monthly schedules – Cycle attribute.
  - Network schedules – Schedules that wait for non-dial-up network access.
  - Network schedules – Date range start and end date attributes.
  - General – Some numeric attributes may have upper limits that are lower than the for earlier releases.

  You can choose not to take pre-upgrade action on schedules that use the obsolete features without losing the schedules in the migration process. The upgrade converts the schedule to a "best fit" interpretation of the original schedule. The Migration Exceptions report discloses any schedule that is altered for a best fit. Refer to "Reviewing Your Reports After Migration" on page 33.

Evaluating Channels and Channel Sets

- Delete channels that are obsolete – The upgrade process migrates all channel assignments and schedule associations. Obsolete channels become clutter in the upgraded environment. Channels that are assigned to client types in the current environment that are not supported in the upgraded environment does not get deleted but does not get associated with a work profile.
- Evaluate your use of folder structures for organizing channels – The new work profile user interface displays the path for any channel or channel set that you include in a work profile. While the view column is subject to resizing, you may want to shorten paths prior to upgrade for easier viewing in the upgraded environment.
- Evaluate your use of the auto-subscribe attribute – Channels or channel sets that have an associated schedule and do not include the auto-subscribe attribute always runs according to the schedule in the upgraded environment. This is changed behavior for Windows clients using Channel Viewer. You may want to remove the schedule if you object to the upgrade behavior.
- Eliminate nested schedules – Channel sets that have an associated schedule do not require any of the channels to have an associated schedule. A channel set that has a schedule will be migrated to become part of a (schedule) monitor-action pair. A channel in a channel set that has its own schedule also becomes part of a different (schedule) monitor-action pair. The result in the work profile is two occurrences of the scheduled channel, once for the channel set and once for the channel.

  Multiple work profiles may result, also with multiple occurrences of the channel, if the channel had multiple assignments.

Evaluating Channel Assignments

Consider taking the following actions to improve your post-upgrade experience:

- Revisit channels with assignments included in channel sets – The upgrade process creates a new work profile for each unique group assignment/client type[1] combination. Any client that was assigned to a channel in a channel set is assigned to a new work profile that includes the channel set. All the group members assigned to the work profile will be authenticated for, and attempt to run, all channels in the set, even if they were previously assigned to fewer than all the channels.

  This change could have significant implications in your Afaria operations, particularly if you organized your assignments by network user group, rather than client group. All members of

1. A client type may include more than one sub-type. For example, the Windows Mobile Professional type includes multiple sub-types such as Pocket PC and Windows CE devices.

the network user group becomes assigned to a work profile attempt to run every channel in the channel set.

- Revisit channels with assignments – The upgrade process creates a new work profile for each unique group assignment/client type combination. Any client that was assigned to a channel is assigned to a new work profile that includes the channel.
- Revisit channels without any assignments – The upgrade process converts channels without any assignments to the allowed channels list in a work profile that is assigned to the system-defined “All Clients” client group. All clients receive this work profile and are allowed to run any of the channels on the allowed channels list.

Reviewing Your Reports After Migration

The Afaria setup program creates migrated profiles. The upgrade process produces the following reports either 1) when it completes n upgrade migration or 2) when you run the upgrade migration utility to evaluate migration results.

- Migrated Items Report – The report contains a list of all the new work profiles produced, the Client assignments, associated client actions, and allowed channels. The report is a Comma-Separated Values (CSV) file, appropriate for import into a spreadsheet application.

  <*InstallDir*>\MigratedItemsReport*N*.txt

  where *N* is a sequential number used to prevent overwriting previous reports

- Migration Exception Report –The report discloses items that needed to be changed as part of the upgrade in order to conform with features and limits in the upgraded environment.

  <*InstallDir*>\MigrationExceptions*NNN*.txt

  where *NNN* is a sequential number used to prevent overwriting previous reports

Refer to "The Upgrade's Migration Activity" on page 29. to learn more about using the migration utility.

Preparing for Palm Documentation Manager Upgrade

Afaria 6.0 introduced changes to Documentation Manager implementation for Palm support. The Afaria product no longer includes a Palm document conversion utility on the Afaria server. Formerly, the utility converted documents prior to deploying them to Palm clients. Also, Afaria no longer delivers a DataViz Documents To Go viewer to the Afaria client.

Consider these changes and the following items for your upgrade planning and operational changes:

- Server-side upgrade
  - The Afaria setup program removes the document conversion utility from the Afaria server. Therefore, you must implement a document conversion method that places device-ready documents into the Document Manager document storage path, as defined in your Afaria server configuration properties.
  - Documents that were previously converted by the document conversion utility are not moved to the new storage location, the Document Manager document storage path, during the upgrade process. Therefore, you must copy them to the new storage location from the following path:
  - <AfariaInstall>\ClientESD\Palm\DocMgr
- Client-side upgrade – Afaria clients that connect to an upgraded Afaria server are automatically upgraded to the new release version. Any existing converted documents and the DataViz Documents to Go doc viewer remain on the client. However for ongoing operations, you are responsible for ensuring that each device has applications installed that can open and view converted documents. Afaria does not supply device-side tools for using the documents.

  The Document Manager client is able to launch a document's associated application only if it can locate an application that is associated with the document's type and "Creator ID".

Preparing for Database Migration

Afaria 6.0 introduced changes to improve logging and query performance. The upgrade impacts the Afaria database tables associated with the following logs:

- Sessions
- File transfer
- Event details

  The upgrade migration action for these tables executes during the Afaria setup program.

The database action is resource intensive and, in the case of large databases, may take longer than 24 hours to complete. During that time, your Afaria server is unavailable for client connections. Therefore, you are strongly advised to take the following actions in advance of executing the Afaria setup program to reduce the amount of time that the upgrade action requires:

1. Change your pre-upgrade Afaria server configuration settings for log cleanup to a value of 5 or fewer days for the following logs:

   - Session log
   - File transfer log
   - Event detail log

   Using the lowest value your operations can tolerate will reduce the amount of data that the setup program must process and therefore, the amount of time that your Afaria server is unavailable for client connections. You may restore your preferred values after the upgrade is complete.
2. Allow the log cleanup server schedule to run, either on demand or according to its regular schedule.
3. Ensure that the log cleanup is complete before starting the Afaria setup program. You can verify log cleanup completion by searching for the “log cleanup completed” log entry in the Messages log.

Preparing Pre-6.0 Clients for Upgrade

For customer who have not yet upgraded to Afaria 6.0, consider the following upgrade information.

Afaria client upgrades occur automatically, using Afaria's Electronic Software Delivery (ESD) feature, as your clients connect to an upgraded Afaria server. Upgrades that fail due to the Afaria platform no longer supporting a client's operating system are recorded in the Messages log.

The upgrade connection performs only an upgrade and does not run requested channels. Use a subsequent connection to continue operations.

Upgrading in the New Profiles Environment

Clients must connect to the Afaria server to receive current profiles. ESD is the preferred method for all Afaria client upgrades. The ESD upgrade process includes an initial connection, during which the client receives all of its assigned work profiles and schedules.

If you choose to reinstall the Afaria Client software using a new client package or need to install new clients, you are advised to include settings for an initial connection in the client package.

API-based Client Connections

An Afaria 5.5 hot fix introduced a new character limit limitation for client APIs using a fully qualified path name for a channel. The length of any ChannelSubsystem FolderItem (channels, channel sets, folders, replication partners, and so on) must be less than 80 characters. The fully qualified path uses syntax:

TransmitterName (or the $root$ alias)\[path...\]ItemName

You are advised to evaluate your existing client API usage prior to installing this release, as this new limit causes connection failures when paths exceed the limit.

Upgrading Clients to a Relay Server Environment

Afaria 6.0 introduced support for using an optional relay server to operate as a proxy for HTTP and HTTPS sessions between the Afaria server and its Afaria clients. Use of a relay server has client upgrade implications that you need to understand in order to make a successful transition

into a relay server environment. Refer to “Setting up a Relay Server” on page 66 for more information.

Starting Setup – Setup Menu Options

Your Afaria license key determines which setup options appear on the setup menu and which are enabled.

1 Close all running programs.

2 Locate the setup.exe file on the root directory of the Afaria product image.

3 Open **setup.exe** to launch the setup program and open the Afaria Setup Menu.

Entering or Updating Your License Key

1 On the setup menu, click **View or Update License Key**.

2 Type your license key into the key box. Choose **Licensing Details** to review your licensing information.

The maximum number of concurrent sessions supported per Afaria server depends on your licensing. The ability to run the maximum number of licensed concurrent sessions depends upon the amount of memory, the speed, and number of the processors on your server.

3 Choose **Apply** to save the license key and return to the setup menu with your licensed options available.

Setup's Install Options

The following install options are available with appropriate licensing:

- **Express Evaluation Install** – This option is only for evaluation licenses. It installs a configured SQL Anywhere database, Afaria Server, and Afaria Administrator on the same server. The server authenticates local users. Refer to "Express Evaluation Install" on page 40.
- **Install** – The installation menu includes the following options:
  - **Server** – Install Afaria server. Refer to "Installing Afaria Server" on page 41.
  - **Administrator** – Install Afaria Administrator. Refer to "Installing Afaria Administrator" on page 53.
  - **Software Manager Tuner** – Install Afaria Software Manager Tuner, an optional Software Manager component. Refer to "Installing Software Manager Tuner" on page 52.

Locating Product Documentation

Product documentation is included on the product installation image.

1 Click **Documentation** on the setup menu to open the documentation menu.

2 Click the item of interest.

- **Readme** – includes information about finding system requirements and release notes on the technical support site and information about what is located on the product installation image.
- **Installation guide** – the English version of *Installing Afaria*. *Installing Afaria* is available in additional languages by clicking on the menu's **Documentation folder** item and navigating the language folders.

  Afaria SMS Integration Suite customers should navigate the documentation folder and use document *Installing Afaria SMS Integration Suite* for installation instructions.
- **Documentation folder** – opens the \Documentation folder on the installation image. The folder includes folders for each supported operating system language's documentation. All product documentation is available in English. Some documents are available in additional languages.

  Afaria SMS Integration Suite customers should use document *Installing Afaria SMS Integration Suite* for installation instructions.

Express Evaluation Install

The express install is valid only for an evaluation license. The express installation performs the following actions:

- Install and configure a SQL Anywhere database[1].
- Install Afaria server its related components with authentication enabled for local users.
- Install Afaria Administrator.

1. On the setup menu, click **Express Evaluation Install**. The program opens the End User License Agreement dialog box.
2. Click **Yes** or **No** to indicate your acceptance or rejection. The installation continues only when you accept the agreement.
3. Specify the account name and password to use to run the Afaria service.

   You must have a user account established for Afaria operations. Revisit topic "User Accounts for Installing and Operating Afaria" on page 11 if you have not completed this prerequisite task.
4. Click **Install**.

1. The Express install includes a 60-day, evaluation copy of SQL Anywhere. You may need to acknowledge one or more informational dialog boxes that describe the evaluation product.

Installing Afaria Server

This section explains how to install the Afaria Server program for the first time, how to install a replication server in an Afaria server farm, and how to upgrade or reinstall an Afaria server. The steps you take to upgrade or reinstall a server are similar to completing a new install. Instructional steps use the following conventions:

(New install) Complete this task for a new install. This includes steps for upgrades or reinstalls that include a new license key.

(Farm install) Complete this task for installing a replication server for a server farm.

(Upgrade or reinstall) Complete this task for an upgrade or reinstall. This includes steps using existing license keys; if you are upgrading or reinstalling Afaria using a new license key, follow the steps for a new install.

Starting the Server Setup Program

Server setup requires that you have your database installed and configured for Afaria, and that you have a user account established for Afaria operations. Revisit the following topics if you have not completed these prerequisite tasks:

- “Configuring Your Database” on page 9
- “User Accounts for Installing and Operating Afaria” on page 11

1. On the setup menu, click **Install**.
2. Click **Server**. The program opens the End User License Agreement dialog box.
3. Click **Yes** or **No** to indicate your acceptance or rejection. The installation continues only when you accept the agreement. Accepting the agreement opens the Welcome dialog box.
4. Click **Next**. See “Selecting the Database” on page 43.

Selecting the Database

Complete the following steps to select your database.

You must have your database installed and configured before beginning this step. Refer to "Configuring Your Database" on page 9.

(New install or farm install) Select one of the following available options:

If you are installing a replication server in a server farm environment, you must select the database for the existing Afaria server to act as the main server.

- **iAnywhere SQL Anywhere**. Select to use the SQL Anywhere database you configured before you installed Afaria, and then click **Next** to continue. Go to "Setting Up SQL Anywhere" on page 43.
- **Microsoft SQL Server**. Select to use the SQL database you configured before you installed Afaria, and then click **Next** to continue. Go to "Setting Up SQL Server" on page 44.
- **Oracle**. Select to use the Oracle database you configured before you installed Afaria, and then click **Next** to continue. Go to "Setting Up Oracle" on page 44.

(Upgrade or reinstall) The install program defaults to your existing database. Verify that the correct database is selected, then click **Next** to continue and have the installation program verify your database settings.

Setting Up SQL Anywhere

If you selected iAnywhere SQL Anywhere, continue with the SQL Anywhere Server Setup dialog.

1 Select your SQL Anywhere server name from the **SA Server Name** list.

The list populates only with names of SQL Anywhere servers on the same subnet. If you need to locate a SQL Anywhere server outside the subnet, select the **Edit Host/Port** check box in order to provide the server information. The **Host** name may be a machine name or IP address.

2 Select a login type:

- **Integrated login**. Select this option to integrate your Windows login with your SQL Anywhere login.
- **SA user login**. Enter the login information for the database user with DBA authority that you created for your Afaria database.

3 Click **Next** to continue.

4 On the SQL Anywhere Server database dialog, type the name of the database you created for Afaria, and then click **Next** to continue. Go to "Continuing Installation" on page 45.

The Afaria installation program validates the database you specify. If you type the database name incorrectly or type the name of the wrong database, you may see a "Request to start/stop database denied" error.

Setting Up SQL Server

If you selected Microsoft SQL Server, continue with the SQL Server Setup dialog.

1 **(New install or farm install)** Complete the following steps:

- Select the **SQL Server** to use with Afaria.
- Select either **Windows Authentication** to use a Windows administrator account with SQL Server privileges or **SQL Server Authentication** to use the SQL Server account with its associated password that you set up for Afaria.
- Click **Next** to continue.

(Upgrade or reinstall) Enter new values or click **Next** to accept defaults and continue.

2 On the SQL Server Database dialog, continue with database definitions.

(New install or farm install) Use the **Select a Database** list box to type or select the database you configured for Afaria, and then click **Next**. Go to "Continuing Installation" on page 45.

(Upgrade or reinstall) Use the **Select a Database** list box to type or select a new database, or accept the default database, and then click **Next**. Go to "Continuing Installation" on page 45.

Setting Up Oracle

If you selected Oracle database, continue with the Oracle Setup dialog.

1 **(New install or farm install)** Complete the following steps:

- Select a driver from the list.
- Enter an **Oracle Service** name.
- Enter your **Oracle User** name for login, then enter your password twice, once in the **Password** area and once in the **Confirm Password** area.
- Click **Next** to continue. Go to "Continuing Installation" on page 45.

(Upgrade or reinstall) Enter new values, or click **Next** to accept the default values and continue. Go to "Continuing Installation" on page 45.

Continuing Installation

Complete the following setup steps to continue the installation.

1 **(New install)** The Confirm Master (or Stand-Alone) Server Install dialog box appears. Click **Next** to continue.

(Farm install) The Confirm Farm Server Install dialog box appears. Click **Next** to continue.

(Upgrade or reinstall) The dialog box that appears depends on whether you are upgrading or reinstalling an existing server farm main server or standalone server, or a replication server in a server farm environment.

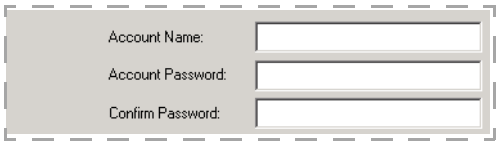
If you are reinstalling the Afaria server as standalone, you must select a new database.

2 The Directory Selection dialog box appears.

(New install or farm install) Click **Next** to accept the default location, or click **Browse** to navigate to a new location. If there is not enough space on your selected install location, a message appears in the window and suggests how to resolve the problem.

(Upgrade or reinstall) The Install Path appears in a read-only view. Click **Next** to accept the default directory location. To change this value, you must uninstall Afaria, then perform a new install.

3 The Service Account dialog box appears.



(New install or farm install) Specify the account name and password to use to run the Afaria service. Click **Next** to continue.

You must have a user account established for Afaria operations. Revisit topic "User Accounts for Installing and Operating Afaria" on page 11 if you have not completed this prerequisite task.

(Upgrade or reinstall) Complete one of these steps:

- To accept the default Service Account information, click **Next**.
- To change the Service Account information, select the **Change existing account information** check box, then enter the Account Name and Password. Click **Next** to continue.

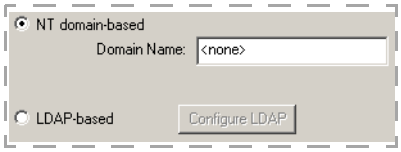
4 The Server Selection dialog box appears. Enter a descriptive name for the Afaria server or click **Next** to accept the default name. Each replication server in a server farm must have a unique name. The server name must not include the backslash (\) character.

5 If you installing a main or standalone server, go to "Selecting Authentication Type" on page 46. If you are installing a replication server for a farm, go to "Completing the Installation" on page 49.

Selecting Authentication Type

Complete the following setup steps to select your user authentication type.

If you are installing a server farm main server or standalone server, or if you are upgrading or reinstalling the server, the Type of Authentication dialog box appears.



(New install) Complete one of the following steps:

- *To authenticate against global Active Directory domain user groups*, select **NT domain-based** and enter the domain you plan to use for authentication and/or assignments. As the administrator, you must also be a member of this domain. Click **Next** to continue. Go to "Completing the Installation" on page 49.

  If you do not choose a domain during installation, you can still add a domain for authentication on the Server Configuration Properties page.

  If you want to allow users to use blank passwords, additional OS settings are required. Refer to *Afaria Reference Manual* | *Platform* > Server Configuration > Properties > "Security" to learn more about the OS requirements for allowing blank passwords.

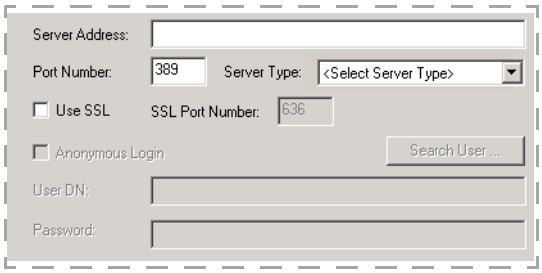
- *To authenticate against the local machine*, keep <none> as the default and click **Next** to continue. Go to "Completing the Installation" on page 49.
- *To authenticate against an LDAP server*, select **LDAP-based** and then click **Configure LDAP**. The LDAP Server Login Information dialog box appears. Continue with "Configuring LDAP Information".

(Upgrade or reinstall) The install program defaults to your original authentication type. Complete one of the steps under New Install to change your authentication type, or click **Next** to accept the default authentication type and continue. Go to "Completing the Installation" on page 49.

Configuring LDAP Information

Complete the following setup steps to configure LDAP settings for your Afaria installation.

1 The LDAP Server Login Information dialog box appears.



Enter the following information:

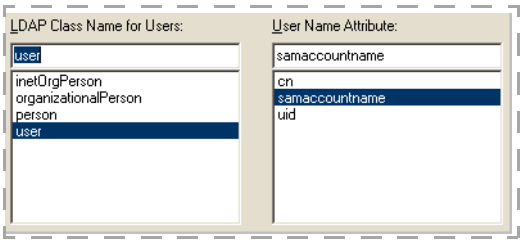
- **Server Address**. Enter your LDAP server address as either a fully qualified domain name such as afaria.mycompany.com or as an IP address.
- **Port Number**. Afaria automatically defaults to the LDAP standard port 389. If you enter another port number, you must enter a number greater than 1024.
- **Server Type**. Select your LDAP Server type.
- **Use SSL**. Select to enable SSL communication with your LDAP server.
- **SSL Port Number**. Define the LDAP server port for SSL communications.
- **Anonymous Login**. Select the Anonymous Login check box to allow the Afaria server to communicate with the LDAP server without using a dedicated LDAP user account for the server. If you select Anonymous Login, you should configure your LDAP server to allow a search of the directory structure for users, user groups, and organizational units and all of their attributes.
- **User DN**. If you did not select Anonymous Login, enter the User DN (Distinguished Name) for the LDAP account the Afaria server uses to communicate with the LDAP server. If you don't know the user name for the account, click **Search User**. You must have an LDAP proxy user configured for an anonymous login to be able to search for users.

  You can enter a name using a wildcard character to search for the correct User DN. For example, you can enter "*mith" or "*mit*" to search for Smith. Select the correct User DN and click **OK** to return to the LDAP Login Information dialog box.
- **Password**. Enter the password for the LDAP account the Afaria server uses to communicate with the LDAP server.

Click **Next** to continue.

2 The LDAP Root Directory dialog box appears. Select a root directory that contains all of the groups, organizational units, and users the server requires for authentication and assignments, then click **Next** to continue.

3 The LDAP User Characteristics dialog box appears.

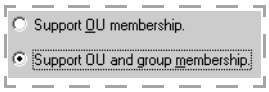


In the LDAP User Characteristics dialog box, select the following:

- **LDAP Class Name for Users**. Select the LDAP Class Name for Users from the list or enter one in the area provided. The user-related Class Names you have created on your LDAP server appear here.
- **User Name Attribute**. Select or enter the user name attribute you use in your LDAP environment. Any name attributes you have configured for your LDAP server appears here. When client users connect to the server, they enter their user ID as the user name you've specified.

Click **Next** to continue.

4 The LDAP Container Settings dialog box appears.



Complete one of the following steps:

- Select **Support OU membership** to assign channels to users based on the organizational unit (OU) to which they belong.
- Select **Support OU and group membership** if you want to assign channels to users based on both the OU and groups to which they belong.

Click **Next** to continue.

Go to "Completing the Installation" on page 49.

Completing the Installation

Continue with the Ready To Start Installation dialog box.

1 Click **Install**.

The Setup Complete dialog box opens when the installation is complete. If during the installation you receive a message that a file is in use, choose one of the following options:

- **Abort**. Quits the installation.

If you are reinstalling Afaria and you click **Abort** to quit the installation, you may find that some of the files were updated and some were not. Run the install program again. If this does not work, uninstall the Afaria Server program and run a fresh installation.

- **Retry**. Close the application using the file specified or close the file in your Windows Task Manager, then select **Retry**. Setup tries to install the file again. If this does not work, select **Ignore**.
- **Ignore**. Continues the process but requires you to restart the computer in order to complete the installation.

You may be prompted to restart your computer when the file copying process is completed. Click **Yes** to restart. The installation program continues from the point at which it was interrupted.

Customers upgrading from a pre-6.0 version may receive informational messages “The parameter is incorrect...” and “Client schedule name: error deleting... “ that inform about the infrastructure migration to the current profiles and policies infrastructure. Supporting information is added to the Migration Exceptions Report. See “Reviewing Your Reports After Migration” on page 33.

2 Select whether you want to start the service at this time.

To allow connections immediately, start the service. To continue with configuring the server, do not start the service.

3 Click **Finish**.

Updating Passwords on the Server

You can change the service account or password associated with the Afaria server or database without running a full reinstallation of the server.

You must close all Afaria programs before updating passwords on the server.

To change the service account or password, use the following command-line switches:

-Maintenance (required)

-ServiceAccount=”name” (optional)

-ServicePassword=”password” (required with ServiceAccount, otherwise optional)

-DatabasePassword=”password” (optional)

You can enter these command-line switches in any order. Note the following examples:

setup -Maintenance -DatabasePassword=”password”

setup -Maintenance -ServiceAccount=”name” -ServicePassword=”password”

setup -Maintenance -DatabasePassword=”password” -ServicePassword=”password2”

The Afaria setup program runs silently. It may take several minutes for the setup to run. You may not know when it has finished unless you watch the task list or run the setup from a batch file. To check for errors, open C:\silent.log.

Reinstalling the Server

You can reinstall the Afaria Server program to:

- Change your database configuration.
- Change the way the server authenticates users.

To change the location where the Afaria files reside, you must first uninstall Afaria and then run a complete reinstall. For more information, see “Uninstalling Afaria Components” on page 87.

If you are reinstalling a standalone Afaria server into a server farm environment as a replication server, the database for that standalone server is orphaned. The new replication server uses the main server’s database. If you are reinstalling a replication server as a standalone Afaria server, you need to create a new database for that server.

If you are uninstalling a replication server from a server farm environment, the process does not automatically delete the database entry for that server. If you plan to reinstall the server, you must delete the server’s entry from the farm’s A_SERVER database table. If you do not delete this server in the database, it continues to appear in the channel replication window in Afaria Administrator as an available server, even though it is no longer an eligible target for replication.

Installing Software Manager Tuner

Software Manager Tuner is an optional Software Manager component.

Use Afaria Software Manager Tuner to customize a Windows Installer Package (.MSI) by creating a separate transform file (.MST) that is delivered and installed with the Package. Once you have used Software Manager Tuner to customize the installation, you'll use Afaria's Software Manager to deliver and install both the package and the transform file at the client. You can install Software Manager Tuner on the same machine as the Afaria server, or you can install it on a standalone computer. If you install the Tuner on the same machine as the server, the installation program checks to see that you have the proper licensing.

1. On the setup menu, click **Install**.
2. Click **Software Manager Tuner** to start the setup program. The program opens the Afaria Software Manager Tuner Install Shield dialog box.
3. Click **Next** to begin the installation. The final InstallShield Wizard dialog box opens at completion.
4. Click **Finish** to close the InstallShield Wizard.

Installing Afaria Administrator

Install Afaria Administrator on the same or different server than the Afaria server.

1 On the setup menu, click **Install**.

2 Click **Administrator**.

3 Click **Next** to continue. The Select Virtual Directory dialog box opens.

If you have already created a virtual directory for Afaria in IIS, select it from the list. If you have not created a directory, type the name for the directory to create it. This directory appears in IIS under Default Web Site.

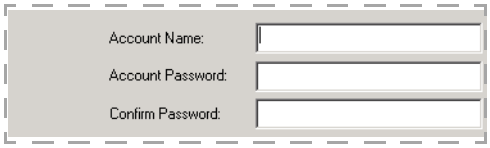
If you create your own virtual directory in IIS before you install Afaria, you must verify that it is properly configured after you install Afaria Administrator. For more information, see "Verifying Afaria Administrator IIS Settings" on page 54.

4 Click **Next** to continue. The Select Physical Directory dialog box opens.

Enter the physical location where Afaria Administrator files should be installed, or click **Browse** to locate the directory.

If you are installing Afaria Administrator on the same machine as the Afaria server, you must install Afaria Administrator in a different directory.

5 Click **Next** to continue. The Specify Credentials dialog box opens.



Specify the account name and password used to run the Afaria service on the Afaria server.

You must have a user account established for Afaria operations. Revisit topic "User Accounts for Installing and Operating Afaria" on page 11 if you have not completed this prerequisite task.

6 Click **Next** to continue. The Domain Selection dialog box opens.

Enter the **Domain name** for the domain from which you select users to administer the Afaria server. To select only from local users, keep the default value <none>.

7 Click **Next** to continue. The Ready To Start Installation dialog box opens.

8 Click **Install** to begin the installation. The Setup Complete dialog box opens at completion.

If during the installation you receive a message that a file is in use, you have the following options:

- **Abort**. Quits the installation.

If you are reinstalling Afaria Administrator and you click **Abort** to quit the installation, you may find that some of the files were updated and some were not. In order for Afaria Administrator to work properly, you should run the install program again. If this does not work, uninstall Afaria Administrator and run a new installation.

- **Retry**. Close the application using the file specified or close the file in your Windows Task Manager, then select **Retry**. Setup tries to install the file again. If this does not work, select **Ignore**.
- **Ignore**. Continues the process but requires you to restart the computer to complete the installation.

You may be prompted to restart your computer when the file copying process is completed. Click **Yes** to restart. The installation program continues from the point at which it was interrupted.

9 The Setup Complete dialog box opens.

10 Click **Finish** to close the installation program. An Afaria Administrator shortcut appears on the desktop.

Verifying Afaria Administrator IIS Settings

If you have problems accessing Afaria Administrator, you should verify if all the correct settings have been applied in IIS. These settings should be automatically set when you install Afaria Administrator.

To verify Afaria Administrator settings in IIS:

1 Open IIS and locate the virtual directory created for Afaria Administratorr.

2 Right-click the virtual directory and select **Properties** on the shortcut menu. The Properties dialog box for the virtual directory you created appears.

3 Ensure this virtual directory has the following settings:

- *On the Virtual Directory page*: Verify the correct path to location where Afaria Administrator is installed; Read and Write access.
- *On the Documents page*: Ensure Default.asp appears in the list.
- *On the Directory Security page*: In the authentication and access area, click **Edit**. The Authentication Methods dialog box appears; ensure the anonymous access check box is clear, and the Integrated Windows authentication check box is selected.

4 To test the virtual directory, select it again in IIS and right-click, then select **Browse** on the shortcut menu. This should launch your browser, and Afaria Administrator should appear. No

server appears in the server list until you have added it. For more information on adding servers to your list, see "Adding a Server to the Server List" on page 57.

If you have stopped and restarted IIS at any time before opening Afaria Administrator, ensure that when you restarted IIS that the WWW Publishing Service also started. If it is not started, you can reset IIS, or you can restart it manually. This service must be running in order for you to open Afaria Administrator.

Changing the IIS Connection Timeout Value

The Default Web Site in IIS has a setting for the connection time out value, which sets the length of time in seconds before the server disconnects an inactive user. You must increase this value so that the Afaria server does not time out its connection with the browser (as it does with the IIS default settings), which results in loss of data.

1. Open IIS and locate Default Web Site.
2. Right-click Default Web Site and select **Properties** on the shortcut menu.
3. On the Web Site property page, in the Connections area, increase the time out value to something greater than the default that meets your needs.

When you increase this value, it changes for all the Default Web Site members in IIS. Ensure you have determined an acceptable value for all sites.

4. Click **OK** to close the Properties dialog box.

Getting Started with Operations

To get started with Afaria, complete tasks that prepare for, and validate, basic operations:

1 Log in a first time using the installing user account context.

2 Add your Afaria server to the server list.

3 Add yourself as a user for:

- Afaria operations
- (Optional) Afaria access policies

4 Return to the default page by clicking **Exit**

5 Log in a second time using your Windows user account.

6 Start the Afaria server.

The workflow covered here provides coverage specific to the getting started goal. Product documentation guide *Afaria Reference Manual | Platform* covers these and other features and tasks in greater detail.

See also:

- "Logging in the First Time" on page 56
- "Adding a Server to the Server List" on page 57
- "Adding Users" on page 57
- "Logging in the Second Time" on page 59
- "Starting/Stopping/Restarting the Afaria Server" on page 59

Logging in the First Time

By default after installation, the only user that can log in to the Afaria Administrator application is the user that installed the product. If you are in a different user context, the application prompts you for the installing user's credentials.

1 Open Internet Explorer and enter the Afaria Administrator address. Syntax: http://<AfariaAdministratorAddress>/<AfariaAdministratorVirtualDir>

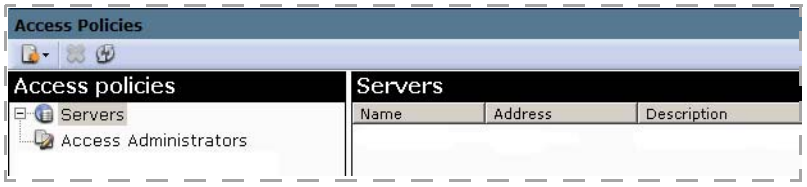
If your current user context is different from the user context for installing the product, then the Enter Network Password dialog opens. Enter the installing user's name, password, and domain and click **OK**. Domain is not required when logging in to a local machine.

The Afaria Administrator server list opens in your browser window without any servers on the list.

Adding a Server to the Server List

The server list is what Afaria users see and choose from when they log in to the product. You must add your server to the list. Use the Access Policies page to add a server. The Access Policies link and page is available only to the installing user and users assigned to the Access Administrator role.

1 On the global navigation bar, click **Access policies**. The Access Policies window opens and the right pane is empty.



1 Right-click Servers in the left pane and select **Add Server**.

2 Type a name, address, and description for the server.

The address can be either an IP or DNS address. The description helps Afaria users recognize named servers.

3 Click **Test Server Connection**.

The test configures the connection, validates the address, and validates whether the server is running.

Adding Users

The Afaria application controls general access to the application by authenticating Windows user credentials. Once a user has general access, it controls access to different features by using roles, to which users are, or are not, assigned.

- Access policies role – role for access to the Access Policies feature, which includes control over role assignments and adding and removing servers
- Server operations roles – role for server operations, such as for individuals who perform administrative operations and provide support for users

By default after installation, the only user with access policy rights is the installing user. By default after adding a server, no user has administrative rights for operations.

For basic operations upon which you can build later, add yourself as a user in roles for:

- Access policies
- Server operations

Adding a User for Access Policies

The product includes a predefined user role called “Access Administrators”. By default, the only user assigned to this role is the installing user. It is defined to enable access to the Access Policies feature, a link to which is located on the Afaria default page when logging in. Users not assigned to this role do not see the link and cannot access the feature.

1 On the Access Policies page’s left pane, select Access Administrator.

2 On the right pane, click **Add**.

The Available Users list box populates with users from the local computer and from any domains that you included during product installation. Both user groups and individual users are included in the list.

3 Select a user or group from the “available” list and move it to the “assigned” list.

4 Click **OK**.

Adding a User for Operations

The product includes a predefined user role called “Administrators”. The role is added, but unpopulated, for each server you add to the server list. It is defined to enable unrestricted, server-specific access to features and commands, excluding the Access Policies feature. Users not assigned to a role for a server do not see that server on the server list when they log in.

1 On the Access Policies page’s left pane, expand the server you defined and select the Administrators role.

2 On the right pane, click the **Users** tab and click **Add**.

The Available Users list box populates with users from the local computer and from any domains that you included during product installation. Both user groups and individual users are included in the list.

3 Select a user or group from the “available” list and move it to the “assigned” list.

4 Click **OK**.

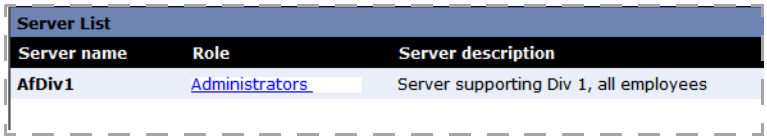
Logging in the Second Time

Log in to Afaria a second time, this time using your Windows user credentials, rather than the installing user's credentials, so you are in the user roles you assigned. You can switch your user context by using the Log In As User feature.

1 From the Afaria default page, click **Logon As User**. The Connect To dialog opens.

2 Supply your Windows user credentials and click **OK**.

The default page opens with content appropriate for your user role. Your user context displays on the banner.



Starting/Stopping/Restarting the Afaria Server

Server/client sessions can run only when the server is started. You can run other operations, such as reviewing logs or reports, performing server configuration, or performing administration and user support tasks when the server is in a stopped or started state. Some configuration changes require restarting the server to take effect.

1 From the Afaria default page, click the role link that is associated with the server to start. The Server Status page opens.

The page includes a dynamic link that changes between "Start Server" or "Stop or Restart Server", depending on the current state of the server.

2 Click the **Start Server** or **Stop or Restart Server** link to open the Current Status dialog. The dialog is dynamic based on the current state of the server and the relevant actions. Click on the appropriate action:

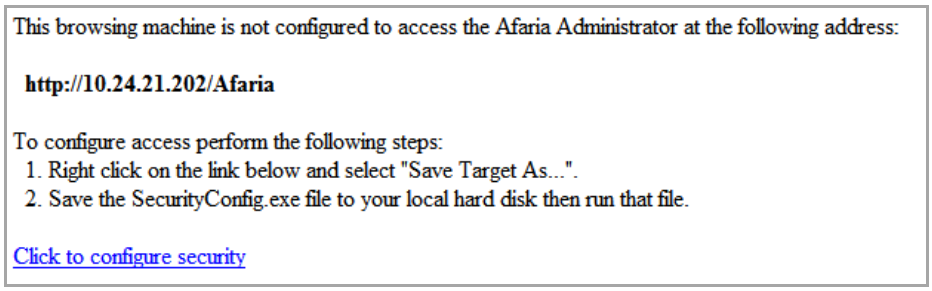
- **Start** – start a stopped server
- **Stop** – stop a started server
- **Restart** – stop then start a started server

Allowing Remote Access to Afaria Administrator

If you plan to view Afaria Administrator via a browser on a remote machine, you must first run this security configuration. Afaria Administrator does not run via a remote browser until you have completed this step.

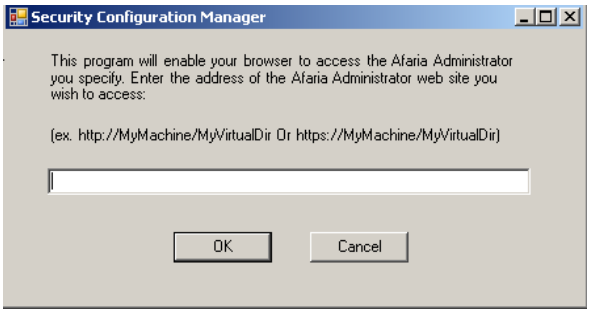
1 Open Internet Explorer and type the address for the Afaria Administrator installation you want to view. Syntax: http://<AfariaAdministratorAddress>/<AfariaAdministratorVirtualDir>

The server list appears briefly, then a configuration message appears in your browser window, similar to the following example:



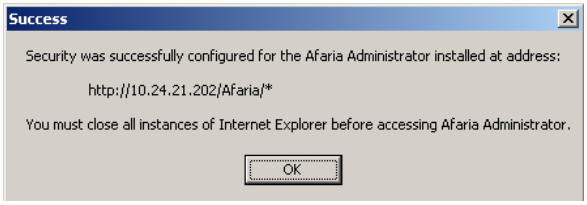
2 Right-click the **Click to configure security** link and select **Save Target As** on the shortcut menu. Save the file to your computer.

3 Open or run the downloaded file. The Security Configuration Manager dialog box appears.



4 Type the Afaria Administrator address according to the format *http://<localhost>/<VirtualDirectory>* and click **OK**. The Success message box should appear.

The address you need to type is the same as the address displayed in the message you received in your browser window.



5 Click **OK** to close the Success message box.

6 Close Internet Explorer.

7 Open the **Afaria Administrator** shortcut on your desktop. Internet Explorer opens and launches Afaria Administrator. The server list appears. It is populated only with Afaria servers for which you have access rights. For more information, see "Adding a Server to the Server List" on page 57.

Configuring the Server

The Server Configuration features let you to define system-wide parameters. This section briefly covers each link in the Server Configuration area. For more details about server configuration, see the *Afaria Reference Manual* | *Platform*.

Server Configuration: Properties

The Server Configuration Properties enables you to define parameters that define client communications, server performance, and settings for optional components.

Properties > **Communication** – Use communication properties to configure parameters for communication sessions with your clients. These parameters include:

- Bandwidth throttling – Increase or decrease the communication rate throughout the course of a client session, allowing client users to run other network applications more effectively when they communicate with the Afaria server.
- Compression – Add files to or view the cache of compressed files that are frequently sent to clients. This reduces connection time and improves system performance.
- Client communication – Use the Client Communication page to define communicating with your Afaria clients including communication protocol, SSL certificate and key, and server address seed value for creating new clients.
- Differencing – Maintain different versions of files that you frequently send to clients; the server sends only the updated bytes of each file in the differencing cache.
- Server identification – Set or change the server's friendly name, which is visible to Windows Channel Viewer clients.

Properties > **Server** – Use server properties to configure parameters for server information and behavior. These parameters include:

- Contact – Provide Channel Viewer users with information regarding the person to contact if they have questions with their client devices or encounter problems during a communication session with the server.
- Failed session cleanup – Control how the system handles failed communication sessions between clients and the server.
- License – View information about your system, including a list of licensed components and client types, the number of licensed sessions, expiration dates (if any), and a brief description of the license type.
- Logging policy – Determine the global logging policy settings. All logs are enabled by default.
- Log cleanup – Specify the cleanup time for the individual logs.
- OMA DM – Define the OMA DM server address properties that OMA DM clients need to communicate with the OMA DM server.

- Security – Configure settings for security measures, including authentication, domain assignments, and client approval. If you are using LDAP for authentication and assignments, you can also enable and configure SSL for LDAP to increase security when you communicate with your Windows clients.
- OTA Deployment Center – Establish settings for Afaria client and Afaria server communication with the OTA Deployment Center.

The OTA Deployment Center must be functional and accessible before you can define it on the property page. See "Setting up the OTA Deployment Center" on page 77.

- SMS Gateway – Define settings for an Afaria Short Message Service (SMS) gateway.
- SMTP – Establish SMTP server settings for your Afaria-initiated, SMTP-based communications.
- User-defined fields – Create new fields in your database tables related to the A_CLIENTS table and read from/write to these fields using the session worklist variables Set Database Field and Get Database Field used for writing to or reading from the database.
- Outbound notification – Control the volume parameters for outbound notification sessions to keep the Afaria server from being overwhelmed with incoming sessions.
- Relay server – Define settings for using a relay server for your Afaria operations. The relay server operates as a proxy for HTTP and HTTPS sessions between the Afaria server and its Afaria clients.

The relay server must be functional and accessible before you can define it on the property page. See "Setting up a Relay Server" on page 66.

Properties > **Component configuration** – Use component configuration properties to configure global settings for installed optional components. These parameters include:

- Backup Manager – Define the physical location for backup storage and define associated log and alert thresholds.
- Document Manager – Apply default location settings for your file selections and settings for alternate media sources.
- Exchange ActiveSync policy – Define a synchronization policy for your enterprise's devices that use Microsoft Exchange ActiveSync to synchronize with your organization's Microsoft Exchange Server. Refer to "About Afaria Access Control for Microsoft Exchange" on page 85 for more information about the feature.
- Manager for SMS – Establish your Microsoft Systems Management Server (SMS) server list and settings for importing SMS packages into the server. When you import SMS packages, Software Manager collects all of the information necessary to create an equivalent Software Manager channel. The new channel can include many of the rich features that a native channel can.
- Patch Manager – Define the location for storing downloaded patches.

Server Configuration: Schedules

Use schedule properties to review and manage system-defined scheduled tasks. The system requires that these tasks execute on a regular basis for ongoing Afaria operations. You can change the schedule for a task or run a scheduled task on demand to suit your needs.

Server Configuration: Client Types

Afaria client types enable you to create and edit custom client types as subtypes to system-defined client types. You may want to create client types for short-term or long-term management purposes. You can create a client type that is defined by the specific operating system, the version, and service packs that have been applied, and so on. You can use these client types when you assign management tasks.

Server Configuration: Alerts

Alert definitions enable you to define and manage which Afaria events—logged actions or conditions relating to your Afaria server, Afaria Administrator, or Afaria clients—raise alerts on your Afaria Administrator. Alerts appear on the Alerts page when the event is detected so you can acknowledge and resolve them. Optionally, you define alerts to notify a contact when some event of interest occurs.

Server Configuration: Tenants

Use the Tenants page to maintain tenant records. A *tenant* is an entity that you can associated with a subset of the client base and its related operations and assets. You must create a tenant record before you can create clients for a tenant or use other multitenancy features.

Server Configuration: License Compliance

The License Compliance page enables you to track software licenses, including their installed versus purchased state on your Afaria clients, their effective and expiration dates, and how

often users run specific applications. This page appears empty until you define software licenses in your database.

Server Configuration: Patch Console

The Patch Console page enables you to view a Microsoft product list and applicable patches that are available download from the Microsoft site. You may use the page to research and select patches for download and initiate the download action. Downloading patches is a prerequisite action for using Afaria Patch Manager to manage patch delivery to your Afaria clients.

The Patch Manager component leverages Microsoft's Baseline Security Analyzer (MBSA) and Windows Update Agent (WUA) technologies to keep your client information current. It requires relevant Microsoft executables for initial and ongoing operations. Refer to *Afaria Reference Manual* | *Platform* for instructions on obtaining these executables.

Setting up a Relay Server

Using Afaria's relay server is not a requirement in your Afaria solution; it is bundled with the Afaria product on the product installation image as an optional component. Therefore, you are not required to complete the procedures described here in order to have a successful Afaria implementation.

Refer to *Afaria Reference Manual* | *Platform* > What is Afaria? > "About the Relay server" to learn more about the relay server, including a diagram and discussion of its components.

Refer to *Afaria Reference Manual* | *Platform* > Server Configuration > Properties > "Relay server" for more information about Afaria server configuration requirements and relay server operations.

Afaria supports using a relay server to operate as a proxy for HTTP and HTTPS sessions between the Afaria server and its Afaria clients. Using a relay server enables you to further secure your enterprise network by moving the session connection point from within your firewall to a location outside of your firewall, to your Demilitarized Zone (DMZ).

The following steps summarize the procedure for installing and configuring a relay server on an existing IIS server:

1. Register the IIS user account on the planned relay server with ASP.NET.
2. Copy relay server files from the Afaria product image to your planned relay server.
3. Create IIS application pools on the relay server.
4. Update the relay server's IIS configuration.
5. Create a relay server configuration file to reside on the relay server.
6. Update your Afaria configuration settings to begin using the relay server.
7. Make your first connection to the relay server.

Register IIS User Account on the Relay Server with ASP.NET

Afaria operations use the relay server's IIS built-in user account named IUSR_<*MachineName*> for gaining anonymous access to Internet Information Services. This account must meet the following criteria:

- have access to the IIS metabase and other directories used by IIS.NET
- be a member of the IIS built-in user group IIS_WPG

To ensure that the account meets the stated criteria, execute the following ASP.NET registration command with the grant access option:

Relay server command path[1]: C:\Windows\Microsoft.Net\Framework\<*Version*>

Command[2]: aspnet_regiis.exe -ga IUSR_<*MachineName*>

Refer to your IIS and ASP.NET product documentation for more information about the IIS user and group and using the registration command.

Copy Relay Server Files

Identify the IIS server that you plan to use as your relay server.

The Afaria product image includes a folder of files that you need for setting up your relay server on an IIS server. Copy folder “ias_relay_server” from your Afaria product image to the IIS server’s home directory (e.g. C:\Inetpub\wwwroot). Ensure that you copy the folder, rather than just the files in the folder.

Copy folder: <product image>\relay_server\ias_relay_server

Create IIS Application Pools on the Relay Server

Use your relay server’s IIS Manager utility to create IIS application pools and application directories for the Afaria Server Web service and the Afaria Client Web service that runs on the relay server. After creating the pools and the application directories, associate each Web service with their respective application pool.

Create a server application pool:

Create an application pool with the following attributes.

- Pool ID – User-defined name.
- Properties

1. If you are operating your IIS server with more than one version of ASP.Net, choose the version that you are using to run your Web site.

2. The command is an example of the registration command with the grant access option that is valid for ASP.Net 2.0.5. The command for your version of ASP.Net may differ.

- Recycling > Recycle worker processes (minutes) – Disabled
- Performance > Idle timeout – Disabled
- Performance > Request queue limit – Disabled
- Performance > Web garden – Set the value to a minimum of twice the number of Afaria servers you are running
- Health > Enable pinging – Disabled
- Health > Enable rapid-fail protection – Disabled

Create an application directory for the server application pool:

1. Select **Web Sites** in the IIS Manager's left pane.
2. Navigate to **Default Web Site** > **ias_relay_server** > **Server** > **Properties** > **Directory**.
3. Create an application directory with the following attributes:
   - Execute permissions – Scripts and executables
   - Application pool – Use the Pool ID that you created for the server application pool

Create a client application pool:

Create an application pool with the following attributes.

- Pool ID – User-defined name.
- Properties
  - Recycling > Recycle worker processes (minutes) – Disabled
  - Performance > Idle timeout – Disabled
  - Performance > Request queue limit – Disabled
  - Performance > Web garden – Set this value to twice the number of Afaria servers you are running, but no less than 5.

    You may want to increase the value if client connections are frequently dropped or if clients experience bad throughput during sessions.
  - Health > Enable pinging – Disabled
  - Health > Enable rapid-fail protection – Disabled

Create an application directory for the server application pool:

1. Select **Web Sites** in the IIS Manager's left pane.
2. Navigate to **Default Web Site** > **ias_relay_server** > **Client** > **Properties** > **Directory**.
3. Create an application directory with the following attributes:
   - Execute permissions – Scripts and executables
   - Application pool – Use the Pool ID that you created for the client application pool

Add Afaria Web service extensions to the IIS Server:

Select **Web Service Extensions** in the IIS Manager's left pane and add the client and server Web extensions to the IIS Server.

1 Add the Afaria Client Web service as a valid extension with the following attributes:

- Extension name – User-defined name for the client extension
- Required files – ias_relay_server\client\rs_client.dll
- Set extension status to Allowed – Enabled

2 Add the Afaria Server Web service as a valid extension with the following attributes:

- Extension name – User-defined name for the server extension
- Required files – ias_relay_server\server\rs_server.dll
- Set extension status to Allowed – Enabled

Update the Relay Server's IIS Configuration

You must run the relay server's IIS adsutil.vbs script to update the IIS server configuration with the application pool changes you have made.

Script location example: C:\Inetpub\AdminScripts

Script command: cscript adsutil.vbs set w3svc/1/uploadreadaheadsize 0

The command returns the current value of the uploadreadaheadsize variable.

Copy the Relay Server Configuration File

A sample configuration file is provided with the relay server files that you copied from your Afaria product image.

Use a text editor to edit the file to match your environment.

Configuration file name: rs.config

Location: <*wwwroot location*>\ias_relay_server\server

The configuration file must contain only ASCII characters.

A copy of the sample is provided here for reference.

Sample configuration file rs.config part 1 of 2[1]

```
#-------------------------------------
# Relay server
#-------------------------------------
[options]
start = auto
verbosity = 1

# Note: When auto start is used, the default log file is
#       <tmpdir>\ias_relay_server_host.log while rshost is active.
#       The value of <tmpdir> is filled using the following environment variables
#       searched in this order:
#             SATMP
#             TMP
#             TMPDIR
#             TEMP

#--------------------
# Relay server
#--------------------

[relay_server]
enable          = yes
host           = 123.45.6.78
http_port       = 80
https_port      = 443
description     = Machine #1 in RS farm
```

1. The actual file is a single, continuous file. The file is represented here in two parts for the sake of page formatting.

Sample configuration file rs.config part 2 of 2[1]

```
#---------------
# Backend farms
#
# Notice that the case sensitive farmID must match the farmID set in the Afaria Administrator's
# relay server configuration page.  Default value in Afaria is farmID=Afaria.
#---------------

[backend_farm]
enable          = yes
id              = farmID
description     = Afaria Farm

#-----------------
# Backend servers
#
# id must match regKey HKLM\Software\Afaria\Afaria\Server\TransmitterId
# on your afaria server
#-----------------

[backend_server]
enable   = yes
farm     = farmID
id       = sc
token    = zyyxpj22p
```

Configuration File Definition

You must restart the relay server engine (rshost.exe) and its supporting components any time you make changes to the configuration file. Refer to "Starting and Restarting the Relay Server" on page 74 for information about restart command.

The relay server configuration file **rs.config** consists of several sections, each indicated by the "[*section*]" convention. Refer to the following definitions for your own configuration file.

- [options] – General options for relay server operations.
  - start – Set value to "auto" to automatically start the relay server engine when an Afaria server connects successfully.

1. The actual file is a single, continuous file. The file is represented here in two parts for the sake of page formatting.

- verbosity – Controls the level of logging. Logs always include errors. Log levels 1-5 always include warnings.

  0 – No logging

  1 – Session-level logging

  2 – Request-level logging

  3 – Packet-level logging, terse

  4 – Packet-level logging, verbose

  5 – Transport-level logging

- [relay_server] – Identifies your relay server and its respective ports for HTTP and HTTPS communications. The relay server's ports must match IIS server's ports.
  - enable – Valid values are "yes" or "no". Set to "yes" to operate the relay server engine and "no" to prohibit relay server operations.
  - host – Relay server's own IP address or host name.
  - http_port – Set value to match the relay server's IIS setting for HTTP communications.
  - https_port – Set value to match the relay server's IIS setting for SSL communications.
  - description – User-defined description for your own reference.
- [backend_farm] – Creates a single, case-sensitive identifier for a single Afaria environment, regardless of whether you are operating a single Afaria server or an Afaria server farm. The farm ID you define in the configuration file must match the farm ID you define in the Afaria Administrator server configuration relay server settings.
  - enable – Valid values are "yes" or "no". Set to "yes" to include the farm in relay server's operations.
  - id – User-defined, case-sensitive value for identifying an Afaria server farm. The default value on the Afaria server configuration properties page for relay server is "afaria".
  - description – User-defined description for your own reference.
  - client_security[1] – Specifies the secure communication protocol requirement for clients connecting to the relay server.

    on – HTTPS is required.

    off – Default. HTTPS is not required; HTTP is a valid connection protocol.

  - backend_security[1] – Specifies the secure communication protocol requirement for Afaria servers connecting to the relay server.

    on – HTTPS is required.

    off – Default. HTTPS is not required; HTTP is a valid connection protocol.

1. This is an optional section that is not represented in the sample. Omitting the section results in the relay server enforcing the default values.

- [backend_server] – Identifies an Afaria server to the relay server. You must have one [backend_server] section for each server in your Afaria environment.
  - enable – Valid values are “yes” or “no”. Set to “yes” to include the server in the relay server’s operations for the farm.
  - Farm – The case-sensitive farm value is the same for each Afaria server. Use the same farm ID as from section [backend_farm].
  - ID – The ID value is unique for each Afaria server. The ID value is defined in each Afaria server’s registry key HKLM\Software\Afaria\Afaria\Server\TransmitterId.
  - Token – The token is any string that you create. Use the same token value for each Afaria server in a farm. The farm token you define in the configuration file must match the farm token you define in the Afaria Administrator server configuration relay server settings.

Configuring the Relay Server to Work with the OMA DM Server

To configure the Relay server, edit the **rs.config** on the relay server by adding a server farm and server ID (which are case-sensitive). An existing server farm can be used. For OMA DM, the server ID must match the OMA DM Server ID as defined in the “Farm ID” field in the Afaria Admin OMA DM server configuration page.

Configuring the relay server assumes that the relay server already exists and is running. For details, refer to the relay server installation and configuration guides.

An example of the **rs_config** file additions, where the backend farm defines the server farm and the backend server defines the server ID:

```
#----------------------------
# OMA DM Server

[backend_farm]
enable       =  yes
id           =  j4farm
description  = J server OMA DM farm

#----------------------------

[backend_server]
enable       =  yes
farm         =  j4farm
id           =  j4oma
token        =  abc
```

After the changes are made and saved to the **rs_config**, restart the relay server.

Configuration File Implementations by Environment

The following environment models indicate the structure of the relay server configuration file you need to match your Afaria environment.

- Single Afaria server – In an environment that includes a single relay server supporting a single Afaria server, the configuration file includes one instance of each section.
- Afaria server farm with four servers – In an environment that includes a single relay server supporting an Afaria server farm with four servers, the configuration file includes the following sections:
  - [options] – one instance
  - [relay_server] – one instance
  - [backend_farm] – one instance
  - [backend_server] – four instances
- Single Afaria server plus an Afaria server farm with four servers – In an environment that includes a single relay server supporting a single Afaria server and an Afaria server farm with four servers, the configuration file includes the following sections:
  - [options] – one instance
  - [relay_server] – one instance
  - [backend_farm] – two instances
  - [backend_server] – five instances

Starting and Restarting the Relay Server

The relay server is configured to automatically start with it's first client connection[1]. This feature is defined when you use the start=auto attribute in the Options section of the configuration file. The relay server reads the current configuration file at each start.

Restart the relay server any time the relay server is already running and you change the relay server configuration file or want to restart the relay server engine. Using the restart command restarts the relay server without restarting IIS and without causing any disruption to other IIS applications.

The following commands assume that you installed the Afaria Server Web service extensions to IIS path inetpub\wwwroot\ias_relay_server\server:

```
CD \inetpub\wwwroot\ias_relay_server\server
```

1. The IIS server must be started before the relay server can start.

rshost.exe -u -qc -f rs.config

You may want to create a batch file for the commands to store in a convenient location in your relay server environment.

Update Your Afaria Configuration

Update your Afaria server and client's configuration settings to begin using the relay server. You need to align several configuration settings with values in the relay server's configuration file. It may be helpful to have a copy of the file for reference.

Refer to *Afaria Reference Manual | Platform* for more information about using the server configuration relay server page to configure Afaria to work with the relay server. The reference describes information for server and client configuration.

Client Upgrade Considerations

Implementing support for using a relay server in an Afaria environment required product development changes to both server-side settings and operations and client-side settings and operations. Therefore, using a relay server has Afaria client upgrade implications. It is recommended that you use the following process to upgrade all clients prior to starting relay server operations:

1. Upgrade the Afaria server.
2. Connect clients to the server to receive a client update.
3. Begin relay server operations.
4. Configure clients for relay server operation using one of the following methods:
   - New client installations – Create new client installation packages with relay server information as the seed data. Install and connect new clients.
   - Update client configuration – Update client configuration settings with relay server information. Connect clients.

Early-Version clients

Client versions earlier than 6.0 cannot connect to a relay server. Either of the following methods can upgrade early-version clients:

- New client installations – Create new client installation packages with relay server information as the seed data. Install and connect new clients.

- Upgrade, then update client configuration – Provide clients with configuration information that circumvents the relay server and connects to the Afaria server directly. Provided that the client version is supported for upgrade to the Afaria server version, the client successfully upgrades. Update client configuration settings with relay server information, and then connect clients.

Client Upgrade Strategy

For customers that are licensed for Session Manager and have clients that require a configuration update to seed relay server connection data, you can automate the client update.

Consider the following upgrade strategy, as described for Windows Mobile clients:

1. Configure the relay server information on your upgraded Afaria server.
2. Create a new client package with relay server seed data.
3. Install the client on test device.
4. Use Session Manager to extract the values for the client's relay server data registry keys HKLM\Software\Afaria\Afaria\Client\Config "RSFarmID" and "RSInfo".
5. Use Session Manager to update the client configuration data for upgraded devices that need the relay server data.

Bypassing the Relay Server

Even after your relay server is operational, the Afaria server continues to support direct client connections. If it is appropriate for your environment, you may allow clients to continue to connect to the Afaria server directly. Afaria clients are still able to initiate connections directly with the Afaria server, bypassing the relay server altogether.

Setting up the OTA Deployment Center

Supported client types – BlackBerry, Palm, Windows Mobile Professional (including Windows CE), Windows Mobile Standard, Symbian, Windows

- Using Afaria's over-the-air (OTA) deployment features is not a requirement in your Afaria solution. Therefore, you are not required to complete the procedures described here for setting up the OTA Deployment Center in order to have a successful Afaria implementation. Afaria also supports deploying Afaria clients using companion PCs, networks, and client APIs.
- Afaria Administrator (Windows IIS Web server) and Afaria OTA Deployment Center (Apache Web server) are typically on separate servers but can coexist if they are configured to ensure that they do not share TCP ports.

The Afaria OTA Deployment Center is a Web server that is a separate component from the Afaria server and Afaria Administrator. It provides software deployment services for your Afaria solution. Setting up the OTA Deployment Center requires that you complete the following manual processes:

1. Install the Apache HTTP server
2. Install the PHP scripting engine
3. Install the PclZip library
4. Install the OTA Deployment Center

Prerequisite Components

The third-party components required for the OTA Deployment Center are not included with the Afaria product. You must obtain the products and licenses directly from their issuing party. Visit the Afaria third-party component dependency reference page, where you can find version information and download instructions for obtaining the required components.

The OTA Deployment Center requires the following components:

- Microsoft Windows, without the IIS server installed or configured; or Linux
- Apache HTTP Server
- PHP scripting engine
- PHPConcepts PclZip, a PHP-based library for accessing zip formatted archives

Installing Apache HTTP Server

The following procedures for installing the Apache server are relevant only if you plan to use Apache on a Windows operating system.

Complete the following procedures to install the Apache server:

1 Use the Windows installer (.msi) to install the server components. Choose the “typical” install option, supplying the specific network, server, and administrator email information for your particular server.

A typical installation installs the binaries, configuration and data files under the “C:\Program Files” folder. If your Windows environment has this folder locked, it may be necessary for you to use the “custom” install option and install to a different location or modify the Apache configuration after the installation is complete. Refer to the Apache documentation for further details.

2 Secure the Apache server. Although there are many methods for securing the Apache server, a minimum recommendation is that you edit the Apache Configuration File (httpd.conf) to turn off the “Indexes” option for the directory root in order to prevent browsing. You can also access the file via the Windows Programs menu or you can locate it in the following path:

C:\Program Files\Apache Group\Apache2\conf

Place a dash (‘-‘) in front of the word “Indexes” from the root directory’s configuration. See the last line in the following excerpt from the configuration file.

```
#
# This should be changed to whatever you set DocumentRoot to.
#
<Directory "C:/Program Files/Apache Group/Apache2/htdocs">

#
# Possible values for the Options directive are "None", "All",
# or any combination of:
#   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
#
# Note that "MultiViews" must be named *explicitly* --- "Options All"
# doesn't give it to you.
#
# The Options directive is both complicated and important.  Please see
# http://httpd.apache.org/docs/2.0/mod/core.html#options
# for more information.
#
    Options -Indexes FollowSymLinks
```

Installing PHP Scripting Engine

The following procedures describe the installation process for a Windows operating system. You must adapt these procedures for a Linux environment.

Complete the following procedures to install the PHP Scripting Engine:

1 Create a new folder named “PHP” under the following path:

C:\Program Files

2 Extract the contents of the PHP distribution zip file to the new folder.

Ensure that the directory structure contained in the zip file is preserved during extraction.

3 Edit the Apache configuration file (httpd.conf) to add the following directives.

LoadModule directives:

```
LoadModule php5_module "c:/Program Files/php/php5apache2.dll"
PHPIniDir "C:/Program Files/PHP"
```

AddType directive:

```
AddType application/x-httpd-php .php
```

4 Create a folder named “Includes” under the following PHP installation folder path:

C:\Program Files\PHP

5 Create a copy of file “php.ini-recommended”, from the root of the PHP installation folder, in the same folder.

6 Rename the copy to “php.ini”.

7 Verify or edit php.ini settings as indicated in the following sample. Many of the required and recommended settings are already set. The convention of bracketed annotations (e.g. [Required]) is introduced only in this sample to provide supplemental information.

```
[Strongly recommended for security] set/verify register_globals=off
[Required] set post_max_size = 32M
[Required] set/verify magic_quotes_gpc=off
[Suggest, security reasons*] set safe_mode=on
Safe_mode_gid=on
safe_mode_include_dir="C:\Program Files\PHP\Includes"
[Recommended for security] set open_basedir="C:\Program Files\PHP\Includes"
[Recommended for security] set file_uploads=off
[Recommended for security] set allow_url_fopen=off
[Required] set extension_dir="C:\Program Files\PHP\ext"
[Required] add extension=php_soap.dll to extensions list
[Required] set soap.wsdl_cache_enabled=1
```

* The setting "set safe_mode=on" requires additional settings if turned on. Please refer to the PHP documentation (including comments in php.ini) for more details.

Installing PHPConcepts PclZip

The following procedures describe the installation process for a Windows operating system. You must adapt these procedures for a Linux environment.

Complete the following procedures to install PHPConcepts PclZip:

1. Extract the contents of the PclZip distribution file into the following path:

   C:\Program Files\PHP\Includes

   This creates a new folder named “pclzip<*version*>”.
2. Rename the folder to “pclzip”.
3. Open the PHP configuration file (php.ini) located in the following path:

   C:\Program Files\PHP
4. Locate the include_path setting that is associated with the Windows path setting. Modify it by removing the leading semi-colon and updating the path value to match your installation’s PclZip path, as shown in the following excerpt.

```
;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Paths and Directories ;
;;;;;;;;;;;;;;;;;;;;;;;;;;;

; UNIX: "/path1:/path2"
;include_path = ".:/php/includes"
;
; Windows: "\path1;\path2"
include_path = ".;C:\Program Files\PHP\Includes\PclZip”
```

Installing the OTA Deployment Center

Installing the OTA Deployment Center requires that you manually copy a collection of source files from the Afaria product image onto the Apache Web server and edit some configuration text files.

About Deployment Center File Types

The deployment center uses the following types of source files for executing different roles in product implementation:

- PHP Scripts – Executable scripts that do not change at runtime.
  - Scripts exposed by the Web server – These scripts are separated into two categories so that you can apply different access permissions to each.
  - Download – Contains one script file (OTADownload.php). This file is referenced by Afaria client download requests. It is suggested that you obfuscate it by making it the default (index) file for the directory. This location must be referenced by the Afaria server configuration properties.
  - Management – Contains the script that implements the Web services used by the Afaria server. This location must be referenced by the Afaria server configuration properties.
  - Deployment center implementation scripts – These scripts are included (used) by the download and management scripts. These scripts are not intended for direct access from the Web server. Direct access is reserved for the PHP script engine, as referenced by the PHP include_path directive.
- Deployment Center data files – Files that are modified by the system at runtime.
  - Database files – Contains information about the set of files published to the deployment center for download. This location is referenced by the deployment center configuration.
  - Deployment files – The set of files published for download to devices. This set of files is determined at runtime through the file publication management functions. There are two classifications of these files:
  - Indirectly accessed – These files are not directly accessible from the Web server, but are served by the download scripts. This location is referenced by the deployment center configuration.
  - Directly accessed – These files are directly accessible from the Web server. They reside in sub-folders under the location of the download script.
- Log files – These files are written by the system for status, audit and debug logging. This location is referenced by the deployment center configuration.

About Deployment Center File Locations

The locations of the various source files that make up the deployment center can be modified. Adapt the following locations to your environment if you are integrating with an existing Web server:

- Script locations:
  - Implementation scripts – <PHP include file root>/iAnywhere/OTA
  - Download scripts – <PHP include file root>/iAnywhere/OTA/download
  - Management scripts – <PHP include file root>/iAnywhere/OTA/management
- Data file locations, located under the implementation scripts directory
  - Database files – <PHP include file root>/iAnywhere/OTA/database
  - Deployment files, indirect access – <PHP include file root>/iAnywhere/OTA/files
  - Deployment files, direct access – Automatically created folders under the location of the download scripts
  - Log files – <PHP include file root>/iAnywhere/OTA/logs

Install the Deployment Center

The following path locations are for a Windows operating system. You must adapt these paths for a Linux environment.

Complete the following procedures if you are installing the deployment center onto a new Web server, rather than integrating it with an existing one.

1. Under the PHP Includes folder (C:\Program Files\PHP\Includes), create the following folders:
   - iAnywhere
   - iAnywhere\OTA
   - iAnywhere\OTA\download
   - iAnywhere\OTA\management
2. Copy files from the Afaria product image to the new folders as follows:
   - \Deployment Center\download*.*
     to C:\Program Files\PHP\Includes\iAnywhere\OTA\download*.*
   - \Deployment Center\management*.*
     to C:\Program Files\PHP\Includes\iAnywhere\OTA\management*.*
   - \Deployment Center\scripts*.* to
     C:\Program Files\PHP\Includes\iAnywhere\OTA*.*

3 Modify the include_path setting in the PHP configuration file C:\Program Files\PHP\php.ini to add the location of the deployment center scripts, as shown in the following excerpt.

```
include_path = ".;C:\Program Files\PHP\Includes\PclZip;C:\Program Files\PHP\Includes\iAnywhere\OTA"
```

This is the same setting modified for the PclZip installation.

4 Add the following excerpt to the end of the Apache configuration file (httpd.conf). The Apache configuration requires using the forward slash mark “/” in path statements for proper implementation.

```
### Afaria OTA Deployment Download and Management script directories
# Set “Options -Indexes” and “DirectoryIndex” to allow
# operation of script by access to directory only.
Alias /Afaria/OTA “C:/Program Files/PHP/Includes/iAnywhere/OTA/download”
<Directory “C:/Program Files/PHP/Includes/iAnywhere/OTA/download” >
Options -Indexes
DirectoryIndex OTADownload.php
</Directory>

Alias /Afaria/OTAmgmt “C:/Program Files/PHP/Includes/iAnywhere/OTA/management”
<Directory “C:/Program Files/PHP/Includes/iAnywhere/OTA/management” >
Options -Indexes
</Directory>
```

About Afaria Access Control for Microsoft Exchange

Afaria Access Control for Microsoft Exchange enables you to add a layer of protection to your Microsoft Exchange Server. The feature filters Exchange ActiveSync device synchronization requests, either by the device's Afaria client status or by the device's status on the Afaria Administrator's Exchange ActiveSync "white list". You can ensure that the Exchange Server is asked to fulfill synchronization requests only from those Afaria clients and white list devices that you choose.

The following steps summarize the procedure for getting started with Afaria Access Control for Microsoft Exchange:

1. Use the Afaria Administrator's server configuration "Exchange ActiveSync Policy" page to define a synchronization policy for your enterprise's devices that use Exchange ActiveSync to synchronize with your organization's Exchange Server.
2. Connect clients to the Afaria server so they can pick up their policy.
3. Install an ISAPI filter on your Microsoft Exchange's IIS server. The filter monitors all Exchange ActiveSync synchronization requests on behalf of Afaria.

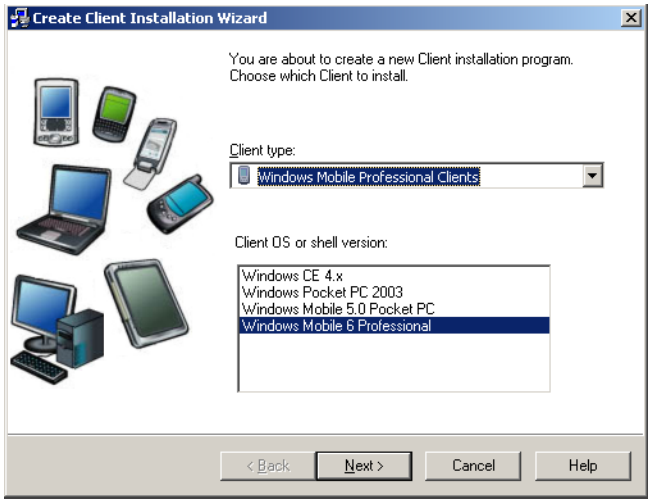
   Refer to *Afaria Reference Manual* | *Platform*, "Server Configuration", "Exchange ActiveSync policy" for more information about getting started with the Afaria Access Control for Microsoft Exchange feature.

Deploying Afaria Clients to Devices

Install an Afaria client on each computing device that you want Afaria to manage. Clients can then connect to the Afaria server to run sessions. Use the Afaria Create Client Installation program to create Afaria client installation packages and then use one of Afaria's deployment methods to get the client onto the computing device for installation.

The Afaria Create Client Installation program is located on your Afaria server.

Start > **Programs** > **Afaria** > **Afaria Create Client Install**



This wizard guides you through creating an Afaria client installation package. Based on client type and your environment, you can choose different options that allow you to deploy the client via a companion PC, a network, or the OTA Deployment Center.

The Afaria Create Client Installation program contains context-sensitive online help that guides you through creating setup files for every device type in your Afaria system. Click the **Help** button on the wizard.

In addition, Afaria includes device-specific files to guide your users through the process of companion-PC-based deployment. The files can be found in the \Documents directory on the Afaria product image.

Uninstalling Afaria Components

You can uninstall Afaria software components by using Add/Remove Programs in Control Panel. Close and stop all Afaria programs and related services to uninstall Afaria server or Afaria Administrator. If you have both Afaria Administrator and Afaria server installed on one machine, you must uninstall both programs. If you want to run only one of these programs, reinstall it. The OTA Deployment Center is an independent component that you need to uninstall separately from the Afaria software components.

If you are uninstalling a replication server from a server farm environment, the process does not automatically delete that server's database entry. If you plan to reinstall the server, you must delete the server's entry from the farm's A_SERVER database table. If you do not delete this server in the database, it continues to appear in the channel replication window in Afaria Administrator as an available server, even though it is no longer an eligible target for replication.

Uninstalling Afaria server deletes the software component and all defined channels but preserves the database.

The most common reasons for the uninstall process to fail are:

- An Afaria program or related service is still running. Stop the programs and related services and run the uninstall program again.
- Windows Explorer or some other program is using at the Afaria installation directory. The uninstall process cannot complete if the directory is in use by any program. Close all programs, then restart the machine and run the uninstall program again.
- One or more of the Afaria system folders is shared by client users. Remove the share from the folder and run the uninstall program again.