
Afaria® Reference Manual Platform

Version 6.5

SYBASE®

Afaria Reference Manual | Platform Version 6.5

Document version 6.50.00

Copyright © 2009 Sybase, Inc. All rights reserved.

Afaria is a trademark of Sybase, Inc. or its subsidiaries. Java and JDBC are trademarks of Sun Microsystems, Inc. All other trademarks are properties of their respective owners. ® indicates registration in the United States of America.

Contents

Preface	10
Afaria support services	10
Chapter 1: What is Afaria?	11
Afaria architecture terms	12
About the Afaria Server	15
Information sharing between peer Afaria Servers	15
About Afaria Administrator	16
About server farms	17
Information sharing within an Afaria Server farm	17
Administration tasks on replication servers	17
About client types	18
Afaria client type – Windows clients	18
Afaria client type – Java clients	18
Afaria client type – Windows Mobile Professional clients	18
Afaria client type – Windows Mobile Standard clients	19
Afaria client type – Palm clients	19
Afaria client type – BlackBerry clients	19
Afaria client type – Symbian clients	19
OMA DM client type	20
About the relay server	21
Relay server components	22
Chapter 2: Using Tenants and Multitenancy	23
Features	24
Using Multitenancy Features	25
Creating Tenants and User Roles for Tenants	25
About the System Tenant	26
Adding New Afaria Clients for a Tenant	26
Adding New OMA DM Clients for a Tenant	27
Actions for Tenants	29
About Naming Items and Assets	30
Sharing an Asset Between Tenants	30
Copying an Asset Between Tenants	31

Actions for Tenant Clients	33
About Upgraded Clients and Assets	34
Web Portal Development	35

Chapter 3: Adding Servers and Users **36**

Logging In	37
Using the Server List	38
Creating Access policies	40
Adding a Server	40
Removing a Server	41
Adding and Removing Users	42
About User Roles	44

Chapter 4: Creating Clients **46**

Creating Afaria Clients	47
About the Afaria client identifier	48
About creating Afaria Client packages	49
About deploying Afaria clients	55
Installing Afaria Client software	56
Starting the Afaria client	58
Updating Afaria clients	60
About your Afaria Windows clients	62
Creating OMA DM Clients	65
Prerequisites for creating OMA DM Clients	65
Creating and managing OMA DM Clients	65

Chapter 5: Home **66**

Server status	67
Active sessions	69
Active session details	70
Alerts	72
View alert details	73
Acknowledge an alert	76
Close an alert	76
View pending alerts	77
Reports	79
Running reports	79
About Creating custom reports	81
Creating custom reports	83
Client deployment	85
Client deployment toolbar	86
Address book properties	87
Distribution list properties	88

Importing addresses	89
Notification templates	91
Sending notifications	101
Self-service portal settings	108
Chapter 6: Server configuration	112
Properties	113
Bandwidth throttling	115
Compression	117
Client communication	119
Differencing	128
Server identification	131
Contact	132
Failed session cleanup	133
License	134
Logging policy	135
Log cleanup	138
OMA DM and Relay Server	139
OTA Deployment Center	142
SMS Gateway	144
Addresses and routing for Afaria messages	150
Security	152
SMTP	158
User defined fields	159
Outbound notification	161
Relay server	163
AV/Firewall	169
Backup Manager	170
Document Manager	171
Exchange ActiveSync policy	172
Manager for SMS	179
Patch Manager	185
Server schedules	186
Client types	189
Add a new Client type	190
Edit Client type properties	192
Alert definitions	193
Define an alert	197
Edit an alert	202
Tenants	204
Adding a Tenant	204
Disabling a Tenant	205
Deleting a Tenant	205
License compliance	206
Create license definitions	206
Set compliance event thresholds	211

Patch console	212
Preparing the patch list	214
Select patches for download	216
Downloading patches for server farms	218
Run patch list synchronization on demand	219
Create Patch Manager alerts	220

Chapter 7: Administration **221**

Profiles	222
About Profiles	223
Managing Profiles	225
Profile – Details	229
Profile – Assignments	231
Profile – Client Actions	233
Profile – Allowed Channels	240
Profile – Policies	243
Group Profile Examples	244
Policies	247
Managing Policies	248
Policy Category – Application Control	250
Policy Category – Antivirus/Firewall	255
Policy Category – OMA DM	259
Client Groups	284
Create a Client group	285
Edit or view group properties	288
Managing and sending outbound notifications	289
Channel Administration	290
Channel Administration Icons	290
Channel and Channel Set Components	292
Running Channels or Channel Sets on Windows Clients	292
Running Channels or Channel Sets on Java Clients	293
Running Channels or Channel Sets on Handheld Clients	293
Channels – Properties Tab	294
Channels – Security Tab	296
Channels – Channels Tab	298
Channels – Profiles Tab	300
Channels – HTML Tab	301
Creating a Channel	304
Creating and Managing Channel Sets	306
Publishing a Channel	307
Editing a Channel	308
Copying a Channel	309
About Importing and Exporting Channels	310
About Outbound Notifications	314
Sending an Outbound Notification	315

Monitors	316
About Monitors	317
Creating a Monitor	321
Editing a Monitor	322
About Hours of Operation	323
Common Monitor Settings	324
Connection Monitor Settings	325
File/Directory Monitor Settings	327
Memory Monitor Settings	329
Power Monitor Settings	331
Process Monitor Settings	332
Registry Monitor Settings	335
Schedule Monitor Settings	337
Window Monitor Settings	344
Channel Replication	345
Replication in a Server Farm Environment	346
Replication in a Server Peer Environment	347
Creating a Replication Set	348
Advertising Channels for Replication	348
Assigning a Server to a Replication Set	349
Registering a Server	350
Viewing General Server Properties	352
Assigning a Replication Set to a Target	352
Setting a Replication Schedule	353
Accepting a Replication Set from a Source	355
Setting Replication Options	356
OMA DM Device Definitions	357
Creating a Device Definition	357
Provisioning a Device	358
Initiating a Client Connection	359
Outbound Notifications	360
Managing client outbound notification addresses	360
Sending an Outbound Notification to Run a Channel	361
Sending an Outbound Notification to Apply Policies	361

Chapter 8: Data views **362**

Database schemas	363
Inventory schemas	364
License compliance schema	388
Creating Custom Database Views	389
Viewing a Custom View's SQL Statement	393
Custom Views and Your Multitenancy Environment	394
Managing Client Data	395
Searching for a Client	397
Revoking and Approving Clients	399
Opening Client Mini-views	401

Viewing Client Properties	409
Changing a Client's Tenant Association	410
Changing a Device ID	411
Deleting Client Data	412
Combining a Client's Afaria Client ID	413
About Outbound Notifications	415
Managing Client Outbound Notification Addresses	416
Sending an Outbound Notification to Run a Channel	417
Sending an Outbound Notification to Apply Policies	418
Client Notifications Status	419
Sending BlackBerry Security Commands	421
Wiping a Remote Device	422
Recovering a Data Security Manager Client Password	425
Managing Data Security Manager Administrator Accounts	431
Creating a New Client Folder	432
Creating a Custom Client View	432
Renaming a Folder or View	432
Viewing Folder or View Properties	433
Creating a Group Within a View	434
Creating a New SQL View Within a View	438
Working with Logged Actions	439
Information Collected by Predefined Views	439
Creating a New Log Folder	445
Creating a Custom Log View	445
Exporting a Log View	448
Working with Client Inventory Data	452
Monitoring Inventory Changes	453
Creating a New Folder in Custom Views	455
Creating a Custom Inventory View	455
Creating a Group within a View	457
Viewing Client Type Inventory Data	462
Acknowledging Monitored Inventory Changes	462
Viewing a Specific Client's Inventory Data	463
Track Software Manager channels	467
View package properties	468
Work with software tracking views	470
Display tracking status views	471
View client status properties	471
How package tracking works	473
Restore backed up client data	477
How hardware and backed up data are represented	478
How clients are represented	479
Selectively restore items to clients	481
Clean up backed up items	481
Tracking Software Compliance and Usage Data	482
Working with Predefined Views	483
Creating a Folder	484
Create a Custom License Compliance View	485

Viewing License Compliance Log Entries	486
Viewing client patch information	487
Making a query	488
Creating a static client group for clients missing patches	489
Creating a dynamic client group for clients missing patches	489
Creating a channel for clients missing specific patches	490
Downloading patches on demand	491
View client deployment information	492
View folder properties and row counts	493
Delete notification information	494
View notification properties	494
View notification batch information	495

Index

496

Preface

This guide is intended for the person responsible for installing and maintaining the Afaria Server. We recommend that you have a working knowledge of your database server, Microsoft Internet Information Server (IIS), Microsoft Internet Explorer and your user directory manager such as LDAP or Windows Active Directory. You also need a working knowledge of the client types you plan to support.

Afaria support services

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

Americas and Asia-Pacific call support:

(678) 585-7320 Atlanta, Georgia

(800) 669-1211 toll-free

European call support:

+44 (0) 1628 50 5321 Maidenhead, Berkshire, UK

0825 800372 toll-free



What is Afaria?

Afaria provides client systems management for remote and mobile computing devices including laptops, desktops, and a wide variety of handheld devices. Use Afaria's powerful tools for automating the business tasks for asset tracking, business productivity, and device and data security. With Afaria, you have the tools to optimize configurations for the different connection types and speeds that all your different computing devices rely upon. IT departments, business executives, and remote and mobile employees all benefit from the streamlined workflow, cost savings, and productivity improvements Afaria provides.

Afaria architecture terms

The Afaria architecture is designed to help manage desktop and mobile computing devices in your enterprise. The following Afaria terms are used throughout the documentation:

- **Afaria Server** – Afaria is a server-based solution that can operate as a single, standalone server or multiple servers in a server farm environment. The Afaria Server communicates with the Afaria database, the Afaria Administrator, the Afaria Over-the-Air (OTA) Deployment Center and Afaria clients. It is the central point for all Afaria activity.
 - **Standalone Afaria Server** – A single Afaria Server operating as the only server in an Afaria installation. The server has a one-to-one relationship with the Afaria database.
 - **Afaria server farm** – Multiple Afaria Servers operating together in an Afaria installation. The servers have a many-to-one relationship with the Afaria database. A server farm includes only one main Afaria server and one or more replication servers. All servers in the farm can access the database and host Afaria client sessions.
 - **Peer Afaria Servers** – Afaria Servers that operate as separate Afaria installations. Peer servers access different Afaria databases and support different sets of Afaria clients.
- **Afaria Administrator, the application** – 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 administrator, the individual** – The Afaria administrator is the person that installs and operates the Afaria product.
- **Afaria clients** – Afaria clients are user devices, such as laptops, handheld devices, and phones that run Afaria Client software. Clients initiate connections with an Afaria Server to run sessions. Servers use sessions to manage the clients and deliver client updates, and to collect data from the client. Several client types are available, depending upon your licensing, so you can choose the one that best suits your users' needs.
- **OMA DM clients** – Open Mobile Alliance (OMA) Device Management (DM) clients are devices that have native support for device management via OMA DM standards and are known to the Afaria Server. You need not install Afaria Client software on devices to use Afaria to manage OMA DM clients; you can create Afaria OMA DM policies and use the Afaria OMA DM server. Afaria OMA DM policies create OMA-DM-compliant messages that accomplish specific management tasks on the device. The OMA DM server runs authenticated sessions with the client to deliver messages. OMA DM policies and server are bundled as an additional-license item.
- **Client type** – Afaria client types aggregate supported devices with like hardware, operating systems, and shells. For example, all Symbian devices are members of the same client type; Windows Mobile Standard devices are members of a different client type. Client types may be further categorized into client subtypes; Windows CE with a specific processor is a subtype of the Windows Mobile Professional client type. Client types are meaningful in Afaria because Afaria components and features may have different capabilities and results for different client types.
- **Groups** – An Afaria group is a collection of one or more Afaria client devices. Manage clients by their group membership, both by their direct membership in a client group and by their

inherited membership as a client device that belongs to a user in a user group. Clients can have membership in more than one group.

- Client group – You can define groups of clients based on their device attributes. For example, you may want to create a group for all of your Windows Vista clients.
- User group – Group defined by their association with a user Afaria can recognize groups of network users, also known as user groups, based on their definition within your organization's computer network. For example, your network may have a user group for all of the service technicians in the East division; the clients belonging to that user group can be managed by the user group.
- Channels – Channels are sets of tasks and instructions that an Afaria client runs when it connects to an Afaria Server. Channels can change device settings, push content out to a client, pull content from a client, or execute other behaviors on a client. Channels types are specialized by component, such as Configuration Manager, Document Manager, Security Manager, and others.
- Monitors – Monitors let you create schedules for clients, and monitor clients for specific client-side activity and data, such as capturing a process start up or determining whether a registry key exists.
- Group profiles – Profiles are the primary mechanism for managing the work performed by groups. The Afaria administrator creates profiles as vehicles for associated policies and work tasks with groups. Profiles primarily include this:
 - Client type – A client type filter limits the types of devices that can use a profile. For example, you can define a profile to be eligible for all Afaria-supported device types, only one device type, or some combination of multiple device types.
 - Assignments – Assignments define the list of groups that receive a profile. Groups that are not explicitly assigned to a profile do not receive the profile.
 - Automated work – Automated work executes without user interaction. Define monitor-action pairs to automate work. A monitor-action pair is a single schedule or other monitor paired with a single action. The paired action may be to connect to an Afaria Server to request a channel, to launch a program, or some other supported action.
 - Allowed work – Allowed work executes when it is requested by a client and is defined as allowed on the profile. Create a list of allowed channels to define the work that the group is allowed to perform.
 - Policies – Policies are focused collections of settings that you can define and enforce on your clients.
- Replication – The Channel replication features enable you to send read-only channel information from a main Afaria Server to its farm servers or send read/write channel information from an Afaria Server to a peer server.
- Tenant, multitenancy – A *tenant* is an entity defined within the Afaria environment that is associated with a subset of the client base and its related operations and assets. *Assets* include nonclient items that support operations, such as profiles, policies, and channels. Tenant features let you maintain clients and assets for multiple tenants. For example, you may want to operate your Afaria installation as a hosting environment to multiple customers or multiple enterprise divisions, with each customer or division assigned to a different tenant identity. *Multitenancy* is the state of an Afaria installation that has the tenant features enabled.

- Relay server – The Afaria solution bundles an optional relay server to operate as a proxy for HTTP and HTTPS sessions between the Afaria Server and its Afaria clients. Using a relay server lets you 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).
- OMA DM server – The Open Mobile Alliance (OMA) Device Management (DM) server is licensed separately from the Afaria Server. It operates as a proxy between the Afaria Server and the OMA DM clients. It runs sessions with known OMA DM clients to serve OMA-DM-compliant messages, as formatted by an Afaria OMA DM policy editor.
- OTA Deployment Center – Afaria supports using an optional Over-The-Air (OTA) deployment center, which is a Web server that you establish to provide software deployment services for your Afaria solution. 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 the Afaria Server

The Afaria Server itself has no user interface. All of the program files reside on the computer where you install the server. This is also the computer that accesses the database. Depending upon your licensing, other Afaria programs that reside on the Afaria Server computer include:

- Channel Viewer user interface – If you are licensed for Windows clients, when you install the server, the Channel Viewer interface is automatically installed as well, enabling you to run Afaria sessions right on the same computer as your Afaria Server.
- Create Client Installation – The Create Client installation wizard guides you through the creation of a client setup file based on the client type. This component is installed on the Afaria Server computer.
- Software Catalog Editor – Afaria’s 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. The catalog includes a listing of most commercially-available applications and user-defined entries that you use to add custom applications to the catalog. You can review software inventory in Data views for inventory and clients. This component is installed on the Afaria Server computer only when you are licensed for Afaria Inventory Manager. For more information on using the Software Catalog Editor, see the online help.
- Over-the-Air (OTA) Publisher – The OTA Deployment Publisher is the Afaria Server conduit to the OTA Deployment Center. Use the publisher to send new client installation packages to the OTA Deployment Center and to manage packages on the center.

Information sharing between peer Afaria Servers

Peer Afaria Servers, that is, servers that do not share a common database, can share information by using export and import features and by using replication.

- Export and import – Information that is exported from one Afaria Server can be imported into another server. You can export these items from a server:
 - Group profiles; including their client schedules and monitors and including referenced channels names but not the associated channel content
 - Channels and their associated content
- Replication – In a peer server environment, replication copies read-write copies of channels from one server to another server. You can define a schedule for executing the replication action to ensure that you keep all replication servers current with changes on the originating server. You can also use replication to emulate a server farm environment; using multiple servers for scalability and fault-tolerance, or to create a distributed server environment.

About Afaria Administrator

Afaria Administrator is the Afaria Server “interface,” a browser-based program that you can access from a computer running a Windows operating system, Microsoft’s .NET runtime, and Internet Explorer Web browser. From the Afaria Administrator interface, you can view important information about the server, configure server properties, manage group profiles, manage policies, and manage Afaria channels.

Afaria > Server List

Server List			
Server List			
Server name	Role	Server description	Server address
AfariaW2k3r2	Administrators	Local system users	10.24.21.202
HelpDesk	Help Desk	Help desk users	Afr1

About server farms

A server farm is a group of servers that act as a single entity. Afaria server farms support the shared use of a centralized Afaria database that contains information about logging, inventory, and alerts data across all servers that are members of the farm. A dynamically elected computer in the server farm is designated as the main Afaria server and it runs the alerts rules engine and the alerts notification, as well as change detection for all Afaria Servers. In a farm environment, the main Afaria server is the server upon which all group profiles, policies, and channels are created, edited and managed. Clients can run sessions with any server in the farm to receive group profiles and request channels. To client users, the integration is seamless.

Information sharing within an Afaria Server farm

Afaria Servers in a farm can share information using the database, and replication.

- Database – Information that is stored in the database is shared by all servers in a farm. The database contains the following, general information:
 - Server configuration data, such as alert definitions and server schedules
 - Afaria clients
 - OMA DM clients
 - Afaria groups
 - Data for data views
 - Group profiles; including their client schedules and monitors and including referenced channels names but not the associated channel content
- Replication – In a farm environment, replication copies read-only copies of channels from the main server to the other servers in the farm. You can define a schedule for executing the replication action to synchronize all replication servers with changes on the main server.

Administration tasks on replication servers

When compared to the main server in a farm, replication servers have limited administration functionality.

- Policies, monitors, channels, and policies – view only
- Replication tasks – not available

About client types

Afaria supports managing a variety of device types. For devices hosting Afaria Client software, device types are categorized as Afaria client types. For devices that are not hosting Afaria Client software, but are OMA-enabled devices that are known to the Afaria Server, device types are categorized as OMA client type.

Afaria client type – Windows clients

Afaria supports using the following types of server interactions for Windows clients:

- Channel Viewer UI – Client users access channels from a Channel Viewer user application that runs on their desktop. Users can perform a variety of tasks including viewing the contents of multiple servers, subscribing to selected channels, and scheduling automatic channel updates.
- Browser UI – You publish channels on a Web page and your Windows client users access the channels using an Internet browser.
- Scheduled mode – The Windows client run channels without according to a schedule that you create. Channels can run transparently and without user interaction.
- Client API – You use Windows client APIs within the context of custom applications to provide client users access to channels.

Afaria client type – Java clients

Afaria supports running channel sessions for desktop Java clients to help you manage your Sun Solaris, HP-UX and Linux client machines.

Afaria client type – Windows Mobile Professional clients

Windows Mobile Professional clients support running channel sessions that take advantage of the rich Windows Mobile platform. Sessions can run either while the client executes a synchronization session with a companion PC or when the client communicates directly with the server over wireless connections. Afaria provides an extensible configuration feature so you can provide provisioning support for devices as they hit the market.

Windows CE clients

Afaria Windows CE client type is a subset of the Afaria Windows Mobile Professional client type. It supports running many of the same channel types and components as the Windows Mobile Professional client type. Exceptions are indicated in the technical support site's release notes; see topic "Client requirements" in the system requirements.



Afaria client type – Windows Mobile Standard clients

Windows Mobile Standard clients support running channel sessions that take advantage of the rich Windows Mobile platform. Sessions can run either while the client executes an ActiveSync session with a companion PC or when the client communicates directly with the server over wireless connections. Afaria provides an extensible configuration feature so you can provide provisioning support for devices as they hit the market.



Afaria client type – Palm clients

Afaria supports running channel sessions for current and legacy Palm OS devices. Sessions can run while the client executes a HotSync session with a companion PC or when the client communicates directly with the server. The software also supports a client version that runs over BellSouth Mobitex used by Palm.net.



Afaria client type – BlackBerry clients

Afaria supports running client software to scan BlackBerry clients for information or issue commands to lock down the client if lost or stolen. You leverage your e-mail environment to collect information such as the number of e-mails stored, the last time it was used, a list of installed software, and more.



Afaria client type – Symbian clients

Afaria supports running channel sessions for Symbian OS devices. Symbian clients bring traditional management strengths into play through full-featured productivity and multimedia devices.



OMA DM client type

Afaria supports using its Open Mobile Alliance (OMA) Device Management (DM) server to send out OMA-DM-compliant messages to OMA-DM-enabled devices that are known to the Afaria Server. Afaria provides a policy editor to create OMA DM tasks that get transformed into OMA-compliant messages. Each Afaria administrator is responsible for assessing the OMA DM capabilities and behavior of the enterprise's devices. To learn more about OMA DM, visit Open Mobile Alliance's Web site, www.openmobilealliance.org and search for the Device Management work group.

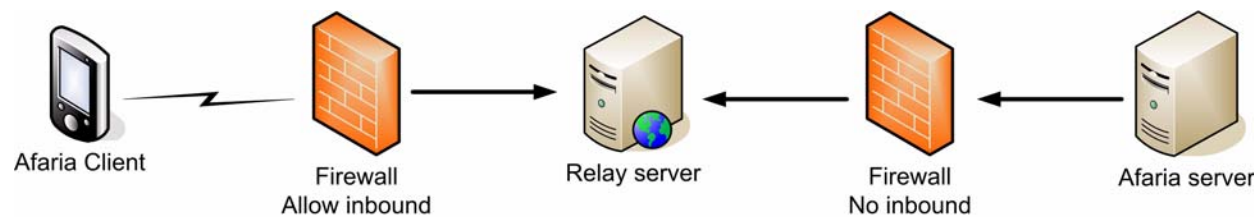
About the relay server



- Use of 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.
- See *Installing Afaria* to learn about relay server and creating its configuration file.

See also “Relay server” on page 163 and “OMA DM and Relay Server” on page 139.

The Afaria solution 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 lets you 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).



When using a relay server, the Afaria clients and the Afaria Server never make a direct connection. The relay server “relays” session traffic from clients to the server and from the server to the clients. The Afaria Server initiates an outbound connection through the enterprise firewall to the relay server and then waits for the relay server to send it session traffic. Afaria clients can initiate a connection to the relay server—as if it were an Afaria Server—and maintain their session with relay server. The relay server continues to relay traffic until the session is complete.

The relay server component may be a single server or it may be a load-balanced server farm. Similarly, the Afaria component is a single Afaria environment, which may be a single server or it may be a farm. Relay servers may be configured to support more than one Afaria environment.¹

1. The Sybase iAnywhere relay server is designed as a scalable solution for supporting a number of Sybase server-based solutions. Afaria is just one example of a supported solution.

Relay server components

Relay server operations include the following executable components:

Relay server outbound enabler (rsoe.exe) – The outbound enabler is the relay server’s agent on the Afaria Server. It is responsible for initiating an outbound connection with the relay server, while sustaining a connection with the Afaria Server. The Afaria setup program installs the outbound enabler. You define its configuration settings by using the Afaria Server configuration properties.

Relay server host engine (rshost.exe) – The host engine resides on the relay server. It is responsible for accepting a single, inbound connection from the Afaria Server outbound enabler; accepting multiple, inbound connections from Afaria clients; and handling the associated processes that occur on the relay server for Afaria sessions. You install the relay server with files that are bundled with the Afaria product. You define its configuration settings by modifying a sample configuration file.

Afaria clients include configuration settings for using a relay server but do not require a separate, executable component.



Using Tenants and Multitenancy

A *tenant* is an entity defined within the Afaria environment that is associated with a subset of the client base and its related operations and assets. *Assets* include nonclient items that support operations and profiles, such as policies and channels. Tenant features let you maintain clients and assets for multiple tenants. For example, you may want to operate your Afaria installation as a hosting environment to multiple customers or multiple enterprise divisions, with each customer or division assigned to a different tenant identity. *Multitenancy* is the state of an Afaria installation that has the tenant features enabled.

Features

Tenant features let you take actions to maintain clients and assets for multiple tenants:

- Add tenants.
- Assign Afaria Administrator users to roles that define which tenants they can administer.
- Add new clients for a tenant.
- Move a client from one tenant to another.
- Use the system tenant as an entity for creating assets to share with all tenants.
- Manage operations and assets, and review data, for a specific tenant.
- Filter Afaria Administrator pages to contain results only for a specific tenant.
- Monitor operations and review data across all tenants.
- Use product APIs and Web services to create your own Web portal for tenant administrators or tenant users to provide access to tenant-specific information.

Using Multitenancy Features

Follow this general work flow to operate your environment with multiple tenants:

- 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 for operations according to your requirements.
 - Assign client groups to profiles, as appropriate for your operations.
 - Add clients to the client groups.
 - Connect clients.

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

Creating Tenants and User Roles for Tenants

Tenants are entities for associating clients and assets, such as profiles and policies, and keeping them separate from other tenant clients and assets. A logged-in user can administer only those tenants selected for his role.

Follow this workflow to add tenants to your system and select tenants for new or existing user roles:

- 1 To create tenants, begin on the Afaria Administrator default page. Click **System Configuration > Tenants** and continue with adding a tenant.
- 2 (Optional) If you want a defined role to have access to fewer than all tenants—all tenants is the default—then select only those tenants you want for the role's tenant list. Begin on the Afaria Administrator default page and click **Access Policies**. Continue with defining a tenant list for a role. You must be assigned to the Access Administrators role to see the **Access Policies** link.

See also [“Adding a Tenant” on page 204](#) and [“Defining a Role's Tenant List” on page 45](#).

About the System Tenant

The multitenancy environment includes a predefined tenant that is named to match the server name you defined during installation. Consider these items about the system tenant:

- It is a valid tenant for operational assets such as profiles, policies, and channels. It is also a valid tenant for clients and client sessions.
- Its assets, other than profiles, are shared with all tenants. Shared assets include:
 - Policies
 - Channels and channel sets
 - Schedules and monitors
- It is the default tenant for the platform-supporting client sessions:
 - Server's Channel Viewer client
 - Replication servers for server farm replication
 - Peer servers for peer-to-peer replication
 - OMA DM server
- It is the default tenant for clients upgrading from a nontenant environment and tenantless clients. A *tenantless client* is one without a known tenant attribute. The system associates clients with the system tenant in these circumstances:
 - The client connects to the server with the system tenant attribute, as explicitly selected during the create client process.
 - The client was created in a nontenant environment, without a tenant attribute, but is connecting to a server in a multitenant environment.
 - The client previously connected to the server with a tenant attribute, but the client's data has since been deleted.
 - The client's tenant attribute does not match any tenants on the server.

Adding New Afaria Clients for a Tenant

Add new Afaria clients (as distinguished from OMA DM clients) for a tenant as required to support your tenant users. Adding new clients for a tenant is a seamless action that occurs

when a client with a tenant attribute connects for the first time. The server associates the tenant attribute with the client at all times, including for active sessions and related client data.

- 1 Create an Afaria Client installation package using the Create Client Installation wizard.

The wizard includes a page for selecting a tenant. Define all other client attributes according to your normal operations.

To create a new package for an existing client, but associate it with a new tenant, delete the client's data from the server before it connects with its new tenant attribute. This action prevents the server from moving the client to the system tenant in an unapproved state when it connects.

- 2 Deploy and install the client packages according to your normal operations.
- 3 Connect the client for a session.

Connecting clients identify themselves with the tenant attribute only during the first session. Client first-time connections are subject to your system configuration security settings for client approval. Therefore, you may have to approve the client for additional sessions.

In some circumstances, the system associates the clients with the system tenant. You can change a client's tenant association by moving it from the system tenant to another tenant.

See also:

- ["Creating Afaria Clients" on page 47](#)
- ["Revoking and Approving Clients" on page 399](#)
- ["Actions for Tenant Clients" on page 33](#)

Adding New OMA DM Clients for a Tenant

Add new OMA DM clients (as distinguished from Afaria clients) for a tenant as required to support your tenant users. Adding new OMA DM clients for a tenant is the same as adding a client in a nonmultitenancy environment, but is done within a specific tenant's context. The tenant attribute is associated with the client when you create the OMA DM client definition record. The server associates the tenant attribute with the client at all times, including for active sessions and related client data.

- 1 On the OMA DM Client Definitions page, set the tenant context to a specific tenant.

Setting the tenant context is an action you take on an Afaria Administrator application page to select a single tenant for your subsequent actions.

- 2 Create an OMA DM client definition record.
- 3 Connect the client for a first time.

The first connection lets the server associate the connecting device to the OMA DM client definition record.

- 4 Add the client to a dynamic client group that is associated with one or more profiles.
- 5 Connect for a second time to run a session according to its profiles.

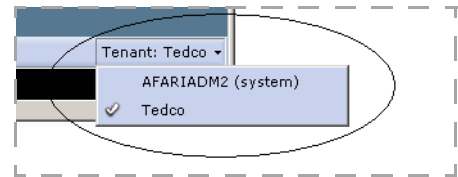
See also:

- [“Creating OMA DM Clients” on page 65](#)
- [“Actions for Tenant Clients” on page 33](#)

Actions for Tenants

The product includes many features for managing operations, only some of which are specific to multitenancy. In addition to adding new clients to tenants and assigning tenants to roles, the following actions are specific to a multitenant environment:

- Set the tenant context for operations and data – Setting context identifies a target tenant for actions and data retrieval in a multitenant environment. Select the appropriate tenant from the tenant selector list on the application’s toolbar. Consider the following items about setting and using the tenant context:
 - Some Afaria Administrator pages, for example, the Active Sessions page, display data for all tenants when you set the context to the system tenant.
 - By default, the system tenant is selected when you open the application. For users in roles that do not include the system tenant, the system selects an alternate tenant.
 - A tenant selection persists as you navigate pages, until you change the tenant context.
 - On non-system-tenant context pages, the system uses italic font to distinguish system tenant assets from other tenant assets. System tenant assets are available for use for all tenants in a read-only state, and are available for editing only in the system tenant context.
- Copy and share assets between tenants.
- Disable a tenant to stop client sessions – Circumstances may dictate that you want to stop all client sessions for a tenant with an option to later restore sessions.
- Delete a tenant from your environment.
- Run reports for tenant operations – You can run reports to review operational data that is not filtered by tenant from your database. For example, you may be interested in reviewing the number and nature of file transfers, for all tenants, in a single report. Many other reports are filtered to run only for a single tenant, based on your current tenant context.
- Define tenant alerts – The system raises an event anytime a client attempts to run a session for a disabled tenant.



See also:

- [“About Naming Items and Assets” on page 30](#)
- [“Sharing an Asset Between Tenants” on page 30](#)
- [“Copying an Asset Between Tenants” on page 31](#)
- [“Disabling a Tenant” on page 205](#)
- [“Deleting a Tenant” on page 205](#)
- [“Reports” on page 79](#)
- [“Define an alert” on page 197](#)

About Naming Items and Assets

The system requires globally unique names for items and operational assets you create. Therefore, you may encounter conflicts when creating, copying, or importing an asset because the asset name exists in another tenant. Items and assets include all things you create and assign a name. For example:

- Client groups
- Client deployment templates
- Profiles, policies, and monitors
- Channels and channel sets, where the name is defined as its complete server path in the channel administration tree

Sharing an Asset Between Tenants

Sharing an asset lets you define and manage one instance of an asset that multiple tenants can use. Assets generally include items such as profiles, policies, and channels; however, profiles are not eligible for sharing. Assets do not include client-specific items such as clients or client groups.

System tenant shared assets are available for use by all tenants. Therefore, for sharing between tenants, create your asset in the system tenant and then use it from whichever tenant you choose.

- 1 Begin in the system tenant context and create a new asset, such as a policy in the system tenant.
- 2 Change to another tenant context on the same asset page. Continuing the previous example, change to tenant X on the policy page.

On non-system-tenant pages, the system uses italic font to distinguish system tenant assets from other tenant assets.

- 3 Use the system tenant policy as you would any of tenant X's policies.

The system tenant is the only tenant that can make changes to the asset. Making changes impacts all the tenants that are using the shared asset.

See also [“Copying an Asset Between Tenants” on page 31](#).

Copying an Asset Between Tenants

Copy an asset between any two tenants to create a new, independent asset in a different tenant. Assets include items such as profiles, policies, and channels, but do not include client-specific items such as clients or client groups.

If an asset is a container for a combination of shared and tenant-specific items, only the system items are subject to copy. For example:

- If the asset is a profile that includes shared monitors and tenant-specific monitors on its client actions list, only the shared monitors persist in the target tenant.
- If the asset is a channel set that includes shared channels and tenant-specific channels, only the shared channels persist in the target tenant.

In both cases, the resulting copy is different from the original and produces different results. You can define new assets in the target tenant to supplement the shared assets and produce intended results.

The steps for copying an asset may vary slightly, based on location in the user interface.

Example – Copying a Profile

- 1 Select the asset in the source tenant's context. For example, set the tenant context to tenant Y and select profile X that you want to copy.
- 2 Right-click the asset and select **Copy to Tenant**.
- 3 Select the target tenant from the tenant list.
- 4 Click **OK**.

The asset is copied to the target tenant's asset page.

Example – Copying a Channel

- 1 Select the asset in the source tenant's context. For example, set the tenant context to tenant Y and select channel X that you want to copy.
- 2 Right-click the asset and select **Copy**.
- 3 Change the tenant context to the target tenant.
- 4 Right-click the target node in the channel tree, such as the server or folder, and select **Paste**.

The asset is copied to the target tenant's asset page.

See also [“Sharing an Asset Between Tenants”](#) on page 30.

Considerations for Copying a Channel

The results for copying channels differ according to several factors, including the type of channel and whether the channel is shared or tenant-specific.

See also [“Copying a Channel”](#) on page 309.

Actions for Tenant Clients

The product includes many features for managing clients, only some of which are specific to multitenancy. In addition to adding new clients for a tenant, the following actions are specific to a multitenant environment:

- Changing a client's tenant association – moves all of the client's history and related data to the new tenant.
- Searching for a client record – is necessary in many instances, including for providing support to a user population that spans multiple tenants. You can search for a client across your entire client database, regardless of whether you know the client's tenant attribute.

See also [“Changing a Client's Tenant Association” on page 410](#) and [“Searching for a Client” on page 397](#).

About Upgraded Clients and Assets

A newly upgraded environment, that is, 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 that you have operating in the preupgrade environment. All upgraded clients and assets, such as profiles and their associated policies and channels, default to the predefined system tenant during the upgrade.

Web Portal Development

You can develop a Web portal that uses product APIs and Web services to access functionality that is otherwise available only through the user interface. You can expose functions filtered by a tenant context, and in doing so, provide tenant administrators, or possibly tenant users, access to functionality that you deem appropriate.

See *Afaria Reference Manual | APIs* for guidance on using the product's automation object model, its objects, collections, APIs, and Web services.



Adding Servers and Users

Add Afaria Servers and Afaria Administrator users to your environment to begin operations. You can add multiple servers to a single Afaria Administrator application, and you can add a user to administer multiple servers.

Logging In

Logging in is a valid action for the user who installed the Afaria Administrator application, and for any user who is already assigned to an access policy role.

- 1 Open Internet Explorer and enter the Afaria Administrator address.

Syntax: `http://<AfariaAdministratorAddress>/<AfariaAdministratorVirtualDirectory>`

Depending upon your current user context, the Enter Network Password dialog may open. Enter either the installing user's, or another valid user's, name, password, and domain and click **OK**. Domain is not required when logging in to a local machine.

The Server List page appears as the default page.

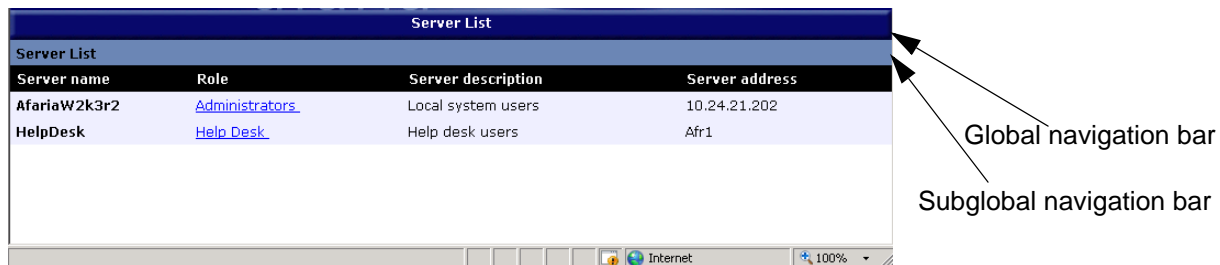
Using the Server List

The server list is the Afaria Administrator application's default page. The page displays the servers in your system to which you have access, depending on your assigned roles. Roles define a user's permissions and rights. Use the Server List page to access some primary functions:

- Access an Afaria Server – Click a role on the Server List page to open a server's Home Server Status page.
- Access the Access Policies page for adding servers, users, and user roles – Click **Access Policies**.
- Change your user context.
- Exit.

See also:

- ["Home" on page 66](#)
- ["Creating Access policies" on page 40](#)
- ["Changing Your User Context" on page 39](#)



The top bar is the *global navigation bar*. Depending on your credentials, you may see two links on this bar: **Server list** and **Access policies**. To move from the Server list page to the Access policies page, click **Access policies**.

The second bar is the *subglobal navigation bar*. On the Server list page, you see one link on this bar: **Logon As User**. Click this link to log off the server in your current user role and log on in a different user role. The Enter Network Password dialog box appears again; enter your credentials to open the Administrator in a new role. The server list page also displays the following information:

- **Server name** – The name of the server with which the current user has a defined user role.
- **Role** – The roles to which the user has access on the Administrator; a role specifies a user's permissions for each area of the Administrator. If a user has not been assigned to a particular role, it does not appear in the list.
- **Server description** – User-defined description. Server descriptions can help users identify which server they want to select.

- **Server address** – The address for the server, expressed either as a fully-qualified domain address or an IP address.

See also [“About User Roles” on page 44](#).

Changing Your User Context

Change your user context when you want to log in with a different set of user credentials without logging off of the server. You can switch your user context by using the Logon As User feature.

- 1 From the Server List page, click **Logon As User**. The Connect To dialog opens.
- 2 Supply your Windows user credentials and click **OK**.

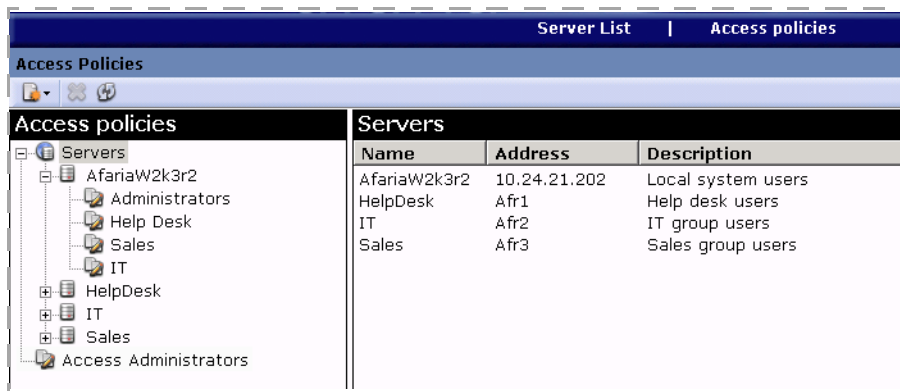
The default page opens with content appropriate for your user role. Your user context appears on the banner.

Creating Access policies

Use the Access Policies page to control access to Afaria Servers. Access policies leverage the Windows user groups security model and let you use roles to control user access to specific servers.

See also:

- “Adding a Server” on page 40
- “Removing a Server” on page 41
- “Adding and Removing Users” on page 42
- “About User Roles” on page 44
- “Creating a Custom User Role” on page 45



Adding a Server

Add an Afaria Server to the list of available servers so you can assign users to the server for operations and support.

The server list is the default page when Afaria users log in to the product. The **Access Policies** link and page is available only to the installing user and users assigned to the Access Administrator role.

- 1 On the Server List page's global navigation bar, click **Access policies**.
- 2 Right-click Servers in the left pane and select **Add Server**.
- 3 Type a name, address, and description for the server.

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

4 Click **Test Server Connection**.

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

Removing a Server

Remove a server when you no longer need to administer the environment or support client users.

- 1 On the Access Policies page, select a server.
- 2 Right-click and select **Remove**.

Adding and Removing Users

Add or remove users to or from user roles to allow or deny access to servers, tenants, and features.



Removing users – If you delete any users or groups in your network, these users can still access the server until you unassign them from all roles.



Adding users – If you did not specify a Windows domain when you installed Afaria, only local groups and users defined on the server computer are eligible for roles.

Adding users from LDAP groups – The API that the product uses to query for LDAP groups can display a maximum of 1,000 results. Therefore, to ensure that any groups you want to use display in your query, add the groups of interest to a custom organizational unit (OU) and name so that it is returned in the first 1,000 results of the query.

Adding a User for Access Policies

Add a user for the Access Policies role to allow the user to administer the server list and user roles.

The product includes a predefined user role called “Access Administrators.” By default, the only user assigned to this role is the installing user. The role enables 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 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

Add a user for an operations role to allow the user to administer or support ongoing operations.

The product includes two predefined user roles called “Administrators” and “Help Desk,” as well as any custom roles you create. The roles are added, but unpopulated, for each server you add to the server list. The Administrators role enables unrestricted, server-specific access to

features and commands. The Help Desk role enables read access to features. Custom roles are user-defined. All operations roles exclude the Access Policies feature.

Users not assigned to any 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 a server and select the target role.
- 2 On the right pane, click the **Users** tab and click **Add**.

The Available Users list 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**.

Removing a User

Remove a user when you no longer need the individual to access a server for operations or support, or to access the Access Policies page.

- 1 On the Access Policies page, select a user role, either the Access Administrator role or a role for a specific server.
- 2 Select the user to remove.
For a user in a server role, click the **Users** tab in the right pane to select the user.
- 3 Click **Remove**.

About User Roles

The Afaria application controls general access to the application by authenticating Windows user credentials. Once a user has general access, access to different features is controlled by roles, to which users are, or are not, assigned. The product includes these types of roles:

- 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 – roles for server operations, such as for individuals who perform administrative operations and provide support for users. Server operations roles are specific to a server and are defined by these attributes:
 - Role definition – the features exposed by the role and the associated right within the feature, defined as read, modify, and create. Create includes delete capability.
 - Users – the users assigned to the role as individual users or as members of a Windows group.
 - (Multitenancy only) Tenants – the tenants exposed by the role. Users assigned to the role have access only to the tenants selected for the role.

By default after installation, the only user with access policy rights is the installing user. By default after adding a server, the installing user is the only user that has administrative rights for operations.

These are the predefined server operations roles:

- Administrator – role for users to whom you want to grant all permissions on the server, including the ability to create, modify, delete, and view all data and reports. A user in this role can execute actions that impact clients.
- Help Desk – role includes limited permissions, including the ability to view all data and reports, but does not include the ability to create, modify, or delete data. A user in this role cannot execute sensitive actions that impact clients and client data, such as a remote wipe or recovering a Data Security Manager password. However, you can modify the role to include these actions. See [“About Role Definition Data Views Create for Support Actions” on page 44](#).

These predefined roles, and any custom roles you create, appear on every server you add to your list.

See also [“Creating a Custom User Role” on page 45](#).

About Role Definition Data Views Create for Support Actions

The role definition Data Views Create attribute is required for any role that must execute:

- Remote wipe
- Outbound notification

- Data Security Manager password recovery



The Data Views Create attribute also lets a user delete client data.

Creating a Custom User Role

Create a custom server operations role when you want to create a role with unique combination of attributes without modifying an existing role.

- 1 On the Access Policies page's left pane, right-click a server and select **Add Role**.
- 2 Define the role's attributes by clicking the associated tab in the right pane and defining the values.
 - **Role definition** – the features exposed by the role and the associated right within the feature, defined as read, modify, and create. Create includes delete capability. Features not included in the definition are not visible to the user.
 - **Users** – the users assigned to the role as individual users or Windows groups.
 - (Multitenancy only) **Tenants** – the tenants exposed by the role. Users assigned to the role have access to data only for the tenants selected for the role.

Custom roles are replicated in each new server you add. Similarly, removing a custom role removes it from every server.

See also [“Adding and Removing Users” on page 42](#) and [“Defining a Role's Tenant List” on page 45](#).

Defining a Role's Tenant List

Support – Multitenancy only

Define a server operation role's tenant list to define which tenants the roles' users can access. Defining the list controls access to a tenant's record, as defined in Server Configuration, and all associated client and asset data.

- 1 On the Access Policies page's left pane, right-click a server and select the target role.
- 2 In the right pane, click the **Tenants** tab.
- 3 Select either **All Tenants** or **Selected Tenants**. For **Selected Tenants**, select any combination of tenants from the list.

A role that is not associated with any tenants still has access to several features that are not tenant-specific, such as: server configuration, alerts, some reports and logs, and channel replication.



Creating Clients

Afaria recognizes two types of clients: Afaria clients and OMA DM clients.

- Afaria clients – Devices that have Afaria Client software installed on a supported computing device in order to communicate with the Afaria Server and run Afaria sessions.
- OMA DM clients – Devices that have native support for device management via OMA DM standards and are known to the Afaria Server by their device definitions.

See also [“Creating Afaria Clients” on page 47](#) and [“Creating OMA DM Clients” on page 65](#).

Creating Afaria Clients

All Afaria client types require having Afaria Client software installed on a computing device in order to communicate with the Afaria Server and run Afaria sessions. Afaria includes the Create Client Installation program that operates as a wizard to allow you to create Afaria Client installation packages for each type of Afaria client. The client's Afaria sessions can begin after you install the client.

The following steps summarize the procedure for creating an Afaria client:

- 1 Create a client installation package.
- 2 Deploy the client installation package to the device.
- 3 Install the client package on the device.
- 4 Start the Afaria client on the device.
- 5 Connect the Afaria client to the Afaria Server to run sessions – Different client types support different kinds of connections. Afaria supports several ways to initiate sessions:
 - User interface command from the device
 - Scheduled, automatic actions
 - Hypertext link
 - Custom programming implementation
- 6 Update the Afaria client when updates are available on the Afaria Server.

See also:

- [“About creating Afaria Client packages” on page 49](#)
- [“About deploying Afaria clients” on page 55](#)
- [“Installing Afaria Client software” on page 56](#)
- [“Starting the Afaria client” on page 58](#)
- [“Updating Afaria clients” on page 60](#)
- [“About your Afaria Windows clients” on page 62](#)

About the Afaria client identifier

Your Afaria solution relies on each of its Afaria clients having a unique client identifier¹ in order to associate all of a client's history, assignments, and related data with a single client computer or device. Installing the Afaria Client software onto a device includes the process that creates the identifier. The client's first Afaria session includes the process that sends the identifier to the Afaria Server. From that point on, all the client's activity is associated with the client record by using the client identifier.

There are some occasions when you may need to remove and then reinstall the Afaria software. Reinstalling the software means that the processes for creating the identifier and sending it to the Afaria Server occur again. Clients that get a new client identifier are new clients in terms of Afaria processes, without any client data. Clients that reuse its previous client identifier continue as existing clients, thereby preserving all their client data.

Afaria Java and Windows clients get a new client identifier when you reinstall. For handheld devices however, whether the client gets a new client identifier or reuses its previous client identifier depends on whether the device is serialized. Installing Afaria software on serialized, handheld device creates a permanent and unique client identifier that is based on the device's serial number and can persist even when a device receives a new Afaria installation. Installing Afaria software on un-serialized devices leaves Afaria without a static reference point, so Afaria creates a new client identifier. Most current-model handheld devices are serialized. However, some device manufacturers do not choose to serialize their devices. Many legacy devices are not serialized.

Combining clients

Afaria includes a feature to allow you reassign a former combine a former client's data with a new client's data. The feature is designed to allow you to manually combine the client data in circumstances when reinstalling the Afaria software creates a new client identifier.

See ["Combining a Client's Afaria Client ID" on page 413](#).

1. The client identifier may also be referred to as the client GUID.

About creating Afaria Client packages

Create Afaria Client installation packages using the Afaria Create Client Installation program. The program is installed on your Afaria Server when you install the Afaria product. The program operates as a wizard. For most client types, you can seed the software with the data required to establish a connection back to your Afaria Server and run Afaria sessions.



Incorrect seeding information can occur on a client after a new client installation is completed in the following scenarios:

- The client synchronizes with a companion PC that has an external seed file, and then receives an OTA deployment notification.
- The client previously received an OTA deployment notification (in SMS message format), and then receives a new notification in other Inboxes. In this case, the previous message in the SMS Inbox takes precedence.

The Create Client Installation program wizard selections are based on user flow and product implementation. Selections may include, but are not limited to, the following items:

- Client type
- Seed data for making a connection to your Afaria Server
- Default channel to run each time the client connects to the server
- Client group assignments
- Service settings and RunAs account information for Windows clients
- Attributes for enabling or disabling user access to configuration settings
- User name and password authentication for running channels that require authentication
- Over-The-Air (OTA) deployment for publishing to the deployment center Web server

Seed data

A new Afaria client relies on connection configuration settings to connect back to the Afaria Server and run its first session. The Create Client Installation program creates seed data and stores it on the client as connection settings.



Incorrect seeding information can occur on a client after a new client installation is completed in the following scenarios:

- The client synchronizes with a companion PC that has an external seed file, and then receives an OTA deployment notification.
- The client previously received an OTA deployment notification (in SMS message format), and then receives a new notification in other Inboxes. In this case, the previous message in the SMS Inbox takes precedence.

Related tasks

Perform the following tasks that relate to using the Create Client Installation program to create your client package:

- Configure your Afaria Server – The Create Client Installation wizard uses some of the server configuration data items as seed data on the client. Ensure that you use Afaria Administrator to complete the following server configuration property pages, as appropriate for your organization and client types:
 - Server identification
 - Client communication
 - Tenants
 - OTA Deployment Center
 - Relay server
 - SMS Gateway
 - SMTP
- Define client groups – Optional. The Create Client Installation wizard prompts you to make static client group assignments for the client package.
- Create channels or channel sets – The Create Client Installation wizard prompts you for the published channel/set that you want the client to run when it runs an Afaria session. You may choose to include channels/sets with group profiles that are delivered to clients upon their first connection.



For some device types supported by Afaria Configuration Manager, you can create and publish a Configuration Manager channel to execute during the client installation, thereby allowing you to establish device settings prior to the client's first connection to the Afaria Server.

- Define monitors – Define monitors for group profiles. Monitors enable you to create schedules for clients and monitor clients for specific client-side activity and data. You may choose to include monitors with group profiles that are delivered to clients upon their first connection.
- Define group profiles – Clients making connections after installing the Afaria client receive their assigned group profiles. You should have group profiles defined in advance of their first connections.



Windows Mobile clients – Clients are seeded with schedules and other supported monitors that are enabled in all profiles to which they are assigned at the time you create the client package. At the time you create the client package, a client's profile assignments include:

- Group profiles that include the All Clients group assignment.
- Group profiles that include any of the static client groups that you select for the client while creating the client package.

See [“Profile – Assignments” on page 231](#) to learn more about group profile assignments and the All Clients group.

- (Optional) Define a network connection or access point on the client – The Create Client Installation wizard may prompt you to specify a specific connection name or access point, as defined on the device, to use to connect to the Afaria Server. The device must already include the definition.



Failure to define a connection or access point may cause the Afaria client to attempt to use an alternate connection or access point when it needs to initiate a connection for an Afaria session. The alternate connection may fail to reach the Afaria Server.



Some devices that are also Sybase iAnywhere Mobile Office clients can use the Afaria Create Client Installation program's pre-defined Desktop Connector setting, if they plan to use Mobile Office's Desktop Connector to connect to an Afaria Server and run Afaria sessions. Look for pre-defined connections in the Create Client Installation wizard.

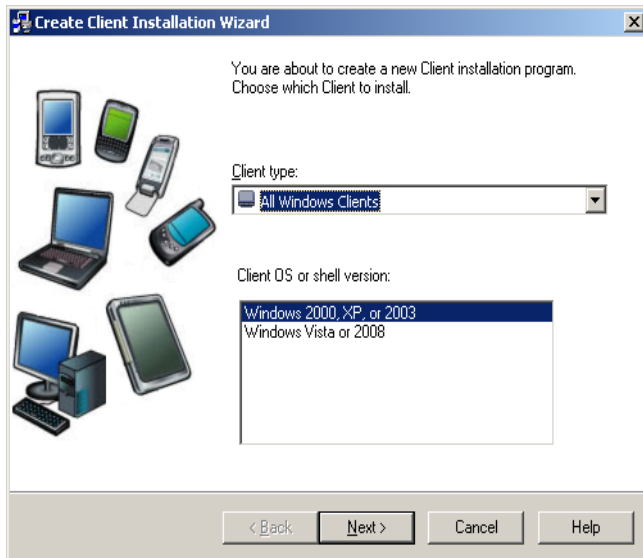
See also:

- ["Server identification" on page 131](#)
- ["Client communication" on page 119](#)
- ["Tenants" on page 204](#)
- ["OTA Deployment Center" on page 142](#)
- ["Relay server" on page 163](#)
- ["SMS Gateway" on page 144](#)
- ["SMTP" on page 158](#)
- ["Client Groups" on page 284](#)
- ["Channel Administration" on page 290](#)
- ["Monitors" on page 316](#)
- ["Profiles" on page 222](#)

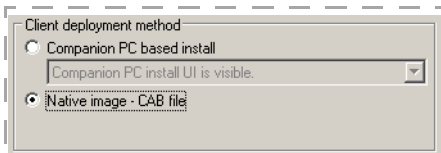
Using the Create Client Installation program

All Afaria Client software is created using the Create Client Installation program on your Afaria Server.

Start > Programs > Afaria > Afaria Create Client Install



Client deployment method

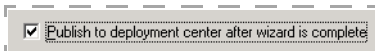


Sample for Windows Mobile

The wizard lets you create Afaria clients in their native file format or packaged in an installation program that is appropriate for the device type.

The sample screen capture illustrates a native image example for a Windows Mobile device. File type CAB is a file type that can be deployed directly onto a Windows Mobile device.

Publish to OTA deployment center



The wizard stores the Afaria Client software in the destination location that you define in the wizard. Additionally, if you select the wizard's check box for deployment center publishing, the wizard also publishes the client package to the Afaria OTA Publisher for over-the-air deployment to devices.

Online help

See the Create Client Installation program's online help for detailed instructions about creating the Afaria Client software for your device. See the Afaria OTA Publisher's online help for detailed instructions on publishing client installation packages to the deployment center.

Alternative client package and seeding for Symbian clients

Afaria provides the Create Client Installation program to create and seed Symbian clients. Afaria also supports an alternative method for client package and seeding that reduces the amount of required user interaction.

The procedure is summarized by the following steps:

- 1 Use the signed Symbian client file (.SIS) as your unseeded client package. Locate the file on your Afaria Server.
`<ServerInstallDir>\ClientESD\Symbian\...`
- 2 Deploy the client to your device using the deployment method of your choice.
- 3 Install the client on the device.
- 4 Send an SMS seeding message to the client.

The client consumes the SMS seeding message automatically and seeds the data.

See also ["About deploying Afaria clients" on page 55](#) and ["Installing Afaria Client software" on page 56](#).

SMS seeding message syntax for Symbian clients

Use one of the following SMS message formats for seeding your installed Symbian client with its server address and default channel.



SMS seeding message syntax must not include any blank characters or blank lines.

- Standard

- Syntax

```
AfOTC_Msg  
[protocol://]Address[:port]  
\Channel
```

where *Channel* is the channel or channel set to request.

- Example

```
AfOTC_Msg  
xnet://65.240.141.130:23002  
\Symbian
```

- Hexadecimal format – Use this format if your carrier corrupts a standard-formatted message. Recognize corrupted messages by observing the device receiving, but ignoring, the message. This format uses hexadecimal characters to represent any special characters that carriers may corrupt.

- Syntax

```
AfOTE_Msg  
[protocol://]Address[:port]  
=5cChannel
```

where *Channel* is the channel or channel set to request.

- Example

```
AfOTCE_Msg  
xnet://65.240.141.130:23002  
=5cSymbian
```

About deploying Afaria clients

Afaria supports a variety of features for you to help you deploy your Afaria client to your device.

- Open Mobile Alliance Client Provisioning (OMA CP) provisioning notification – For OMA-CP-enabled devices, Afaria provides notifications that permit provisioning a device with specific network configuration settings.
- OTA deployment notification – The Afaria OTA Publisher lets you publish Afaria client installations, called packages, by pushing them out to an associated deployment center Web server. You use Afaria to send out an OTA notification to a device. The OTA notification typically includes instructions and a link, in the form of a URL, for downloading and installing the Afaria client.
- Companion PC – For handheld devices, the Afaria Create Client Installation program can produce the client that is ready to be delivered to the device via the PC that hosts its desktop synchronization software. You can deliver the Afaria client to the companion PC and the user can use the synchronization software to install it on the device.
- Custom method – Use a custom application or method for deploying the Afaria client. The Afaria Create Client Installation program lets you create Afaria clients in their native file format or packaged in an installation program that is appropriate for the device type.

Your deployment options for using Afaria deployment features may vary based on device type, capability, and its current state.

- Windows computer – Run the Afaria Client installation program from a known location on a local area network, local drive, or portable media; or via a browser.
- Java computer – Deliver the Afaria client file from a known location on a local area network, local drive, or portable media; or via a browser.
- Handheld devices, OMA CP capable and not configured for connectivity – Configure device connectivity settings using an Afaria OMA CP configuration notification, and then use Afaria OTA deployment to deploy the client.
- Handheld devices, OMA CP incapable and not configured for connectivity – Manually configure connectivity settings, and then use Afaria OTA deployment to deploy the client.
- Handheld devices, with a companion PC – Deliver the Afaria client to the user's companion PC, and then the user uses their companion PC to deploy the client.
- Handheld devices, already configured for connectivity to the Afaria Server – Use Afaria OTA deployment to deploy the client.
- All devices – Custom method for delivering the Afaria client to the device in the device's native format.

See also [“Client deployment” on page 85](#).

Installing Afaria Client software

In order for your end users to access and execute the Afaria Server, they must install the Afaria Client software on their device. The process for installing the client software varies by client type.

Install handheld client software

The process for installing the client software varies by the delivery method.

Install via companion PC

To assist your device users with installing the Afaria client on their device via their companion PC, your Afaria product image includes several device-specific files that you can distribute with the client installation package that you created using the Afaria Create Client Installation program.

Locate the files in the product image's \Documents folder.

Install via OTA deployment

The Afaria client downloads onto the device after the device holder visits the OTA deployment center's download page and chooses the link for their download. Once downloaded, the client launches the installation process. The device holder may have to respond to messages on the device to complete the installation.

Install on BlackBerry devices

Consider the following items related to installing Afaria Client software on BlackBerry devices:

- Installing on BlackBerry clients requires that you allow for third-party applications to install on the device. BlackBerry Enterprise Server (BES) includes this setting as a configuration item. You must ensure that this setting is at least temporarily set to allow third-party applications to install at the time that you plan to complete the client install. You can change the configuration setting after the Afaria client installation is complete.
- Different carriers may require different levels of user intervention at install time and the first time that you exercise Afaria functionality.

Install Windows client software

Windows client users need only to run the executable file on their PC to install the product. The client user interface contains online help to assist end users with tasks.

Installing Java client software

The Java client type is an exception to the other Afaria client types in that its Afaria Client software is deployed to the client as a predefined, unseeded file (.TAR) that is the same for all Java clients. The file is a collection of scripts, functions, and methods that you unpack and execute to leverage existing functions and methods that are native to the Java platform.

Use the following procedure to install the Java client onto a Java computer:

- 1 Copy file `<JavaClient>.tar` file to the client computer.
- 2 At the client's command prompt type `tar -vxf <JavaClient>.tar`, then press **Enter**. The .tar file creates a temporary directory called `Afaria_inst` and unpacks the files into that location.
- 3 Navigate to the `Afaria_inst` directory.
- 4 Type `sh ./AfariaInstall` to execute the Java client installation script. This script creates the hidden directory `.Afaria`, establishes support for Netscape Browsers, and sets appropriate file permissions.

Installation is complete. The client user can now run the Java client.

Starting the Afaria client

Windows and handheld Afaria clients start when the device is powered on. If the Windows Afaria client is installed as an application, rather than service, you can start the user interface by choosing **Afaria > Afaria Channel Viewer** on the Windows program menu.

The process for starting Java Afaria clients varies by the way you want to run the client: with or without a user interface.

Running the Java client with a user interface

Running the Afaria Java client with a user interface initializes a status window for viewing session activity. Use the following procedure to run the client with the user interface:

- 1 Use Afaria Administrator to create a Session Manager channel for a Java client with the “Generate HTML parameter file” attribute enabled on the HTML property page. Afaria creates a parameter file (.xec) on the server.



See “Channels – HTML Tab” on page 301 for more on using the HTML property page.

- 2 Copy the .xec file to the Java client.
- 3 Open the home directory on the client and type the following command:

```
.AfariaLaunch java -jar .Afaria/Afaria.jar -f <path/XEC filename>
```

Running the Java client without a user interface

Running the Afaria Java client without a user interface suppresses client messages and provides a way to run silent sessions. Use the following procedure to run the client without the user interface:

- 1 Use Afaria Administrator to create a Session Manager channel for a Java client with the “Generate HTML parameter file” attribute enabled on the HTML property page. Afaria creates a parameter file (.xec) on the server.
- 2 Copy the .xec file to the Java client.
- 3 Open the home directory on the client and type the following command:
- 4 Optional. You can use the following command (one continuous command) to suppress client messages and route them instead to an output file:

```
.AfariaLaunch java -jar .Afaria/Afaria.jar -f <path/XEC filename> -n
```

```
.AfariaLaunch java -jar .Afaria/Afaria.jar -f <path/XEC filename> -n  
output.txt
```

Starting the Java client's outbound notification listener

Execute commands from the \$HOME directory for default Afaria locations.

Start the listener to listen on default port 3005:

```
java -cp .Afaria:..Afaria/Afaria.jar .Afaria/Listener
```

Start the listener to listen on an alternate port:

```
java -cp .Afaria:..Afaria/Afaria.jar .Afaria/Listener nnnn
```

Updating Afaria clients

The Afaria Server maintains a repository of the most current Afaria Client software and channel component files. These files may change after server upgrades, licensing changes, feature pack installations, and hot fix installations. The server uses Electronic Software Delivery (ESD) methods to deliver file updates to connecting Afaria clients that require them. The process for updating Afaria Client software varies by client type.

Afaria updates for handheld clients

The beginning of each client session includes a check to see if the server has file updates for the client to apply. The Afaria ESD feature automatically delivers the file updates and the client automatically applies the updates without requiring any user interaction.

Afaria updates for Windows clients

The beginning of each client session includes a check to see if the server has file updates for the client to apply. The Afaria ESD feature automatically delivers the file updates. How the client retrieves and applies the updates depends on the value of the following Afaria Server registry key that is installed during product installation:

`hklm\software\afaria\afaria\server\silentupgrade`

The key is defined according to the following values:

- 0 – Not silent.
- 1 – Silent, attended reboot. Prompts client user for reboot.
- 2 – Silent, unattended reboot. No prompting.
- 3 – Obsolete key. Defaults to behavior of value 5.
- 4 – Silent, no reboot. If upgrade requires reboot, the process is aborted. This key is included only for backwards compatibility and should be used with caution.
- 5 – Silent, delayed reboot. If reboot is necessary, waits until the client user performs a reboot to continue the upgrade process.

Update to upgrade Windows client



If a reboot is required and your client user connects to the server before rebooting, the upgrade process is incomplete and the Afaria client will not run a session but the server will create a log entry.

When Afaria's Electronic Software Delivery (ESD) applies an upgrade for the Afaria Windows client a system restart may be required to fully complete the upgrade, such as when files are in use by the operating system or other components. If the user defers the system restart until a later time, and then attempts to run a session, Afaria will display a brief message to the client user that the system must be restarted before running any sessions. After the user restarts the client system, and the upgrade is completed, all sessions will run normally.

Data Views > Logs – When a client in need of a restart attempts to run a session, a message is added to the server log to record the event. Administrators can use the log message to identify clients in need of a reboot. To access the log, open the Afaria Administrator application and then choose **Data views > Logs > Messages > All**. Search for a message "...<ClientName> needs to reboot to complete ESD update".

Afaria updates for Java clients

Updating Java clients is a two-connection process:

- 1 Run the following client command to connect to the server and download all ESD updates to the .Afaria/Update directory:

```
<ClientInstallDir>/AfariaLaunch java -jar <ClientInstallDir>/Afaria.jar -f  
<path/XEC filename>
```

- 2 Run the following client command to connect to the server and apply the ESD updates:

```
<ClientInstallDir>/AfariaLaunch java -jar <ClientInstallDir>/Afaria.jar -f  
<path/XEC filename>
```



Client updates may fail if the Afaria outbound notification listener is running. Stop the listener when updating your Afaria client by using the stop command that is appropriate for your operating system.

About your Afaria Windows clients

Afaria Windows clients are supported for many of Afaria's platform and component features. As is the nature of device management in general, and Afaria components in particular, successful operations depends in part on your understanding of how the Windows client is designed to operate in the Afaria environment.

The following topics discuss some aspects of operating an Afaria Windows client.

Windows OS variations and Afaria operations

The different Windows OS versions that Afaria supports use different native APIs, .NET Framework technologies, and have differences in user and application security and management. These differences significantly affect the execution of some Afaria operations as well as the results they produce.

Afaria is designed to install and operate in different contexts: as logged on user, as a service without associated user credentials, and as a service with associated user credentials. This flexibility lets you manage Windows computers in ways that best suit your enterprise.

While it is your responsibility to understand the behavior of each Windows OS version that you use in your organization, the variations in Windows OS versions warrant advisement about some of the Afaria behavior impacted by the differences. Consider the following subjects as you plan and manage Afaria Windows client operations for different Windows OS versions.

Client installation and data storage

- Client installation and data directory – Windows OS versions vary with respect to the security restrictions enforced when writing application data to the Program Files folder. Therefore, Afaria Windows clients use different implementations for storing install files and data files based on Windows OS version.
 - Windows Vista client default install folder – %PROGRAMFILES%\Aclient\Bin
 - Windows Vista client default data folder – %ALLUSERSPROFILE%\Aclient\Data
 - Windows pre-Vista clients install and data folder – %PROGRAMFILES%\Aclient
- Session variables – You may want to use session variables <ClientDataDir> and <ClientOS> during operations to help you decide upon and execute behavior that is appropriate for different OS versions.
- Client install package and client installation
 - Windows Vista – Within the User Access Control (UAC) security framework, the client is installed with the LOCALSYSTEM account and does not require a set of credentials to run an application as a service. The Afaria Create Client Installation program does not prompt for user credentials when you create a package for a service client.

- Windows pre-Vista – The security framework for running an application as a service optionally permits associating user credentials with the service operations. The Afaria Create Client Installation program does prompt for optional user credentials when you create a package for a service client.

Channel operations – Software Manager, Session Manager, Patch Manager

Channels often need to perform tasks that require elevated privileges in order to be successful. You need to understand the interrelationship between the Afaria client context, the operating system security restrictions on specific channel tasks, and the channel's features you choose. It is the interrelationship of these items that impacts a channel's ability to successfully execute.

- Afaria client context – The Afaria client service or user context for performing channel tasks:
 - Afaria client installed as a service without associated administrator credentials
 - Afaria client installed as a service with associated administrator credentials
 - Afaria client installed as the logged on user
- Operating system security restrictions – The operating system may restrict or limit channel tasks at the client. These restrictions may vary by Windows OS version.
 - Write to the root folder
 - Write to the Windows folder
 - Write to the Windows system folder
 - Write to the registry
 - Interact with the user interface

Channels include features and options that enable you to work successfully within the operating system security framework.

- Software Manager features
 - Expose or suppress user interface interaction
 - Attach answer-response files
 - Define command-line parameters for launching an executable
 - Supply the channel with credentials that impersonate a user
 - Automatically launch an installation or uninstallation process
- Patch Manager features
 - Install property “select reboot mode”
 - Install property “impersonation”
- Session Manager features
 - Read, write, and delete files and folders

- Get, set and delete registry values
- Impersonate user events
- Execute programs and scripts
- Expose message to user interface event
- Use and set session variables
- Use and read environmental variables

Windows browser client

Afaria supports creating HTML-based channels—as one option for creating channels—that Windows clients can execute via a Web browser. Windows clients that run a channel this way are referred to as Afaria browser clients. Browser clients may also run non-HTML channels.

Browser clients in a server farm

Afaria browser clients may warrant special consideration in an Afaria server farm environment. By default, browser clients connect only to the main Afaria server. If you feel it is necessary that you distribute browser client connections across your farm environment, then you can force the distribution by using a round robin load balancer.

Channel Viewer in a Multitenancy Environment

Channel Viewer is an optional application for Windows clients. It provides a user interface for Afaria operations that you choose to expose to your users. The interface includes a view for servers, folders, and channels. In a multitenancy environment, all of the system tenant's folders are exposed to all Channel Viewer users, regardless of their tenant association. The folder is empty for the user unless you add an item to the user's group profile.

Creating OMA DM Clients

OMA DM Clients are devices that have native support for device management via OMA DM standards and are known to the Afaria Server by their device definitions. You need not install Afaria Client software on the device to manage OMA DM Clients. You must, however, create Afaria OMA DM policies and use the Afaria OMA DM server.

Prerequisites for creating OMA DM Clients

Before creating OMA DM Clients, complete these server configuration tasks:

- Configure the Afaria SMS gateway
- Configure the Afaria OMA DM server

See also [“SMS Gateway” on page 144](#) and [“OMA DM and Relay Server” on page 139](#).

Creating and managing OMA DM Clients

The workflow for managing OMA DM Clients is summarized by the following steps:

- 1 Create an OMA DM device definition and have it connect to the OMA DM server.
- 2 Add the OMA DM Client to a static group.
- 3 Create OMA DM policies for device management.
- 4 Create a group profile with the following attributes:
Assignments – Add the static group
Policies – Add the OMA DM policies
- 5 Connect the Clients again to receive their assigned group profile and any associated policies during the session.

See also:

- [“OMA DM Device Definitions” on page 357](#)
- [“Client Groups” on page 284](#)
- [“Managing Policies” on page 248](#)
- [“Policy Category – OMA DM” on page 259](#)
- [“Initiating a Client Connection” on page 359](#)



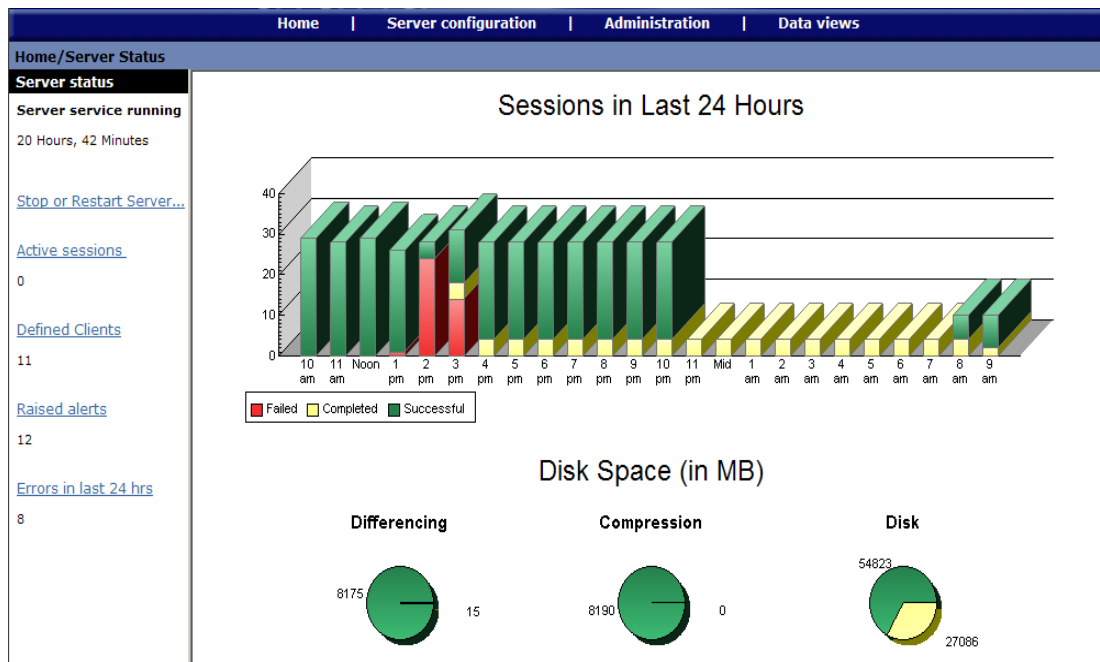
The Home area of the Afaria Administrator contains pertinent information about your Afaria Server, such as the number of client sessions you have run in the last 24 hours, the number of active communications clients are currently running with your server, and the number of defined clients on your server. The Home area displays information about raised and pending alerts on your server, and provides the ability to generate, view and print reports about client sessions and inventory, server logs and messages, client deployments and other important information about your Afaria Server.

This chapter covers these topics:

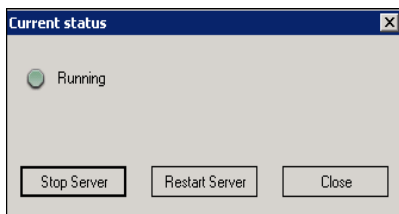
- [“Server status” on page 67](#)
- [“Active sessions” on page 69](#)
- [“Alerts” on page 72](#)
- [“Reports” on page 79](#)
- [“Client deployment” on page 85](#)

Server status

When you click a server link on the Afaria Server list page, the Home page for that server appears and defaults to the server status. This page displays all of the client sessions (Failed, Completed, Successful) that have occurred in the last 24 hours, as well as the disk space for your server, Compression cache, and Differencing cache.



In the left navigation pane, you can select the following links:



- Stop or restart Server** – Clicking this link displays the Current Status dialog box, which allows you to stop the server service. You use this same option to restart the server service when it is stopped.
- Active sessions** – This link takes you to the Active sessions page, which allows you to view client communication sessions in real-time, as well as details about any session you select. The number of current active sessions appears below the link; if no sessions are currently running, the number shows as zero (0).
- Defined Clients** – Select this link to go to the Data Views, Clients page, which displays a list of all defined clients in your system. The number of defined clients appears below the link; if you have not yet defined any clients, the number shows as zero (0).
- Raised alerts** – Select this link to go to the Alerts page, where you can view any raised alerts on your server. The number of current raised alerts appears below the link; if no raised alerts exist on your system, or if you have not defined and enabled alerts on your system, the number shows as zero (0).

- **Errors in last 24 hrs** – Select this link to go to the Alerts page to view any errors that have occurred within the system in the last 24 hours. The number of any errors that have occurred within the last 24 hours appears below the link; if there have been no errors, the number shows as zero (0).

Active sessions

The Active Sessions page displays all active client sessions in your system in real-time. To view the Active sessions page, click **Home** on the global navigation bar and select **Active sessions**. The Active Sessions window is dynamic; as client sessions run, the information that appears changes. To view static information about client sessions, view the Sessions folder in Data views, Logs, or view the Session Log Report in Home, Reports.

Home Server configuration Administration Data views							
Home/Active Sessions							
Active sessions							
User	Client	Address	Channel	Status	% compl...	Throughput	Throttling state
automation	AUTO07	10.24.24.45	NA	CONNECTING		.0 Kbps	Disabled
automation	AUTO07	10.24.24.45	NA	CONNECTING		.0 Kbps	Disabled
automation	AUTO07	10.24.24.45	Win32Load	Send 1.2mb.zip	70%	499.7 Kbps	Disabled
automation	AUTO07	10.24.24.45	Win32Load	Send 500k.zip	52%	334.3 Kbps	Disabled
automation	AUTO07	10.24.24.45	NA	CONNECTING		.0 Kbps	Disabled
automation	AUTO07	10.24.24.45	Win32Load	Send 1.2mb.zip	96%	461.3 Kbps	Disabled
automation	AUTO07	10.24.24.45	Win32Load	Send SAMPLES.XLS	96%	126.1 Kbps	Disabled
automation	AUTO07	10.24.24.45	Win32Load	Get checkmem.exe		261.2 Kbps	Disabled
automation	AUTO07	10.24.24.45	Win32Load	Send checkmem.exe	100%	76.5 Kbps	Disabled
automation	AUTO07	10.24.24.45	NA	CONNECTING		.0 Kbps	Disabled
automation	AUTO07	10.24.24.45	NA	CONNECTING		.0 Kbps	Disabled
automation	AUTO07	10.24.24.45	NA	CONNECTING		.0 Kbps	Disabled
automation	AUTO07	10.24.24.45	Win32Load	Wait dummy.txt		432.1 Kbps	Disabled
automation	AUTO07	10.24.24.45	NA	CONNECTING		.0 Kbps	Disabled
automation	AUTO07	10.24.24.45	Win32Load	Send 1.2mb.zip	100%	368.0 Kbps	Disabled
automation	AUTO07	10.24.24.45	Win32Load	Send 500k.zip	100%	391.4 Kbps	Disabled
automation	AUTO07	10.24.24.45	NA	CONNECTING		.0 Kbps	Disabled
automation	AUTO07	10.24.24.45	NA	CONNECTING		.0 Kbps	Disabled
automation	AUTO07	10.24.24.45	Win32Load	Send 1.2mb.zip	20%	391.4 Kbps	Disabled
automation	AUTO07	10.24.24.45	Win32Load	Get checkmem.exe	0%	299.3 Kbps	Disabled
automation	AUTO07	10.24.24.45	NA	CONNECTING		.0 Kbps	Disabled
automation	AUTO07	10.24.24.45	NA	CONNECTING		.0 Kbps	Disabled
automation	AUTO07	10.24.24.45	NA	CONNECTING		.0 Kbps	Disabled

The Active Sessions page displays the:

- **User** – Name of the user currently logged on or authenticated at the client that is currently running the channel communication session.
- **Client**. User name, as defined on the client.
- **Address** – IP address of the client currently running the channel.
- **Channel** – Name of the channel currently running at the client.
- **Status** – The event type currently executing at the client, such as SEND or GET.
- **% Completed** – The percent completion of a specific file transfer event. This number does not represent the progress of an entire session.
- **Throughput** – The current throughput, in kilobytes per second, for any active client sessions. This value includes consideration for file transfers occurring during the session and all data exchanged during other session events.
- **Throttling state: threshold: [average]: [target]** – The average threshold and the target threshold for the current active session.

For OMA DM Clients, the OMA DM server appears in the active sessions list instead of the client because the OMA DM server runs sessions¹ with the Afaria Server as a proxy for the client. OMA DM Client information is available in the active session details.

Multitenancy users

Setting the tenant context to the system tenant displays active session for all tenants, rather than just the system tenant.

Active session details



View additional details about a current active session by selecting the session in the Active Sessions page and clicking **Properties** on the toolbar. The information that appears in the Active Session Details window is dynamic; it changes as the session runs.

The screenshot shows a window titled "Active session details" with two main sections: "Session information" and "Event information". Each section contains a table with two columns: "Session information" or "Current event information" and "Value".

Session information	
Session information	Value
Channel	InvMgr - Hardware Scan
Start time	10:00:18
Status	CONNECTED
Throughput	3.5 Kbps
Throttling state	Disabled

Event information	
Current event information	Value
Event #	0
of total events	101
Start time	10:00:27
Channel	InvMgr - Hardware Scan
Command	
Server path	InvMgr - Hardware Scan
Client path	
File date	
File size	
Bytes transferred	
% complete	

A "Close" button is located at the bottom right of the window.

While the server communicates with clients, you can view details about events that are executing, including information on channel and event-level completion status and a progress indicator for file transfer commands.

1. The OMA DM server leverages the architecture in the Windows Channel Viewer client that is installed on the Afaria Server. Therefore, you may observe Channel Viewer system tray activity during OMA DM server sessions.

The Session information area displays the following information about current sessions:

- **Channel** – The channel currently running at the client.
- **Start time** – The time the connection began for this channel.
- **Line status** – Indicates if the resource is busy by displaying CONNECTING or CONNECTED.
- **Current throughput** – The current throughput, in kilobytes per second, for any active client sessions. This value is likely to peak and become most relevant during file transfer events, and drop during nontransfer events.
- **Throttling state** – The state of bandwidth throttling for current sessions.

The Event information area displays the following information about current sessions:

- **Event # of total events** – The currently executing event number and the total number of events.
- **Start time** – The starting hour, minute, and seconds for the current event.
- **Channel** – The channel to which this event belongs.
- **Command** – The command that the event is processing,
- **Server path** – The associated server parameters for this event. If the event involves files, then the parameters are likely to be file names. If the event accepts additional parameters, those parameters appear, even though they are not files. The “Server Path” heading does not change for each event.
- **Client path** – The associated client file and path for this event. This field is blank if the event does not involve a file.
- **File date** – When an event involves a file, this field displays the “last modified” date and time associated with this file. Otherwise, the field is blank.
- **File size** – The total number of bytes in the file being transferred. This field is zero (0) if the event does not involve a file.
- **Bytes transferred** – The number of bytes successfully transferred. This value also influences the % completion information.
- **% Complete** – The percent completion of a specific file-transfer event. This number does not represent the progress of an entire session.

Click **Close** to return to the Active Sessions page.

Alerts

The Alerts page allows you to view raised alerts on your Afaria system. These alerts notify you when some incident arises on your Afaria Server, server components, or clients, so you can acknowledge and resolve it quickly. In a farm environment, the alerts engine runs on all computers in the farm, but only *one* computer in the farm responds to an alert; this computer is dynamically elected. The first server to start up in a farm scenario will run the alerts engine; if that computer goes down for any reason, another server will run the alerts engine and respond accordingly to any raised alerts. This ensures that any events on your system will be handled at any given time.



All Afaria Servers in a farm environment must be configured in the same manner, or servers may not respond correctly to raised alerts. For more information on configuring alerts, see [“Configure alert options” on page 194.](#)

You can access the Alerts page three ways: click Home on the global navigation bar and select Active sessions on the drop-down list; click **Alerts** on the subglobal navigation bar; or click the **Raised alerts** link in the left pane of the Home page.




Alerts are made up of a series of events that cause the alert to be raised; you select the events that trigger alerts. No alerts will appear on the Alerts page until you have defined and enabled them; for more information on defining alerts, see [“Alert definitions” on page 193.](#)

You can acknowledge the alert by selecting its check box; acknowledging an alert does not close the alert. Acknowledging the alert simply lets other people viewing the alert know that someone is aware of the alert; it also stops the system response to the alert. If the alert you want to acknowledge does not appear in the window, you can use the Find alert box to type the name of the alert and then click **Find alert**. You can also complete a wildcard search. If the alert for which you are searching has been raised on the server, it will appear in the window.

Home Server configuration Administration Data views					
Home/Alerts					
Find alert					
Alerts					
Raised alert	Description	Time opened	Time acknowledged	State	Contact
<input type="checkbox"/>	Maximum Number of A Specific...	A specific registered alert...	12/2/2008 2:53:58...		Unacknowledged
<input checked="" type="checkbox"/>	A Custom Alert	User defined custom alert...	12/2/2008 2:57:08...	12/2/2008 3:36:16...	Acknowledged
<input checked="" type="checkbox"/>	Alerts Console - A specific re...	A specific registered alert...	12/2/2008 2:53:58...	12/2/2008 3:36:21...	Acknowledged
<input checked="" type="checkbox"/>	Backup Manager - Final disk ...	The final used disk space ...	12/2/2008 2:56:08...	12/2/2008 3:36:26...	Acknowledged
<input checked="" type="checkbox"/>	Backup Manager - Initial disk ...	The initial used disk spac...	12/2/2008 2:57:53...	12/2/2008 3:36:28...	Acknowledged
<input checked="" type="checkbox"/>	Backup Manager - Middle disk...	The middle used disk spac...	12/2/2008 2:57:53...	12/2/2008 3:36:31...	Acknowledged
<input type="checkbox"/>	Backup Manager - Pending re...	A backup cannot proceed...	12/2/2008 2:57:53...		Unacknowledged
<input type="checkbox"/>	Client - Client diff cache full	The Client File Differenc...	12/2/2008 2:57:44...		Unacknowledged
<input type="checkbox"/>	Client - Client diff cache high	The Client File Differenc...	12/2/2008 2:57:43...		Unacknowledged
<input type="checkbox"/>	Client - Client diff cache low	The Client File Differenc...	12/2/2008 2:57:42...		Unacknowledged
<input type="checkbox"/>	Client - Client diff cache medi...	The Client File Differenc...	12/2/2008 2:57:43...		Unacknowledged
<input type="checkbox"/>	Configuration Manager - Cont...	The user exports the dat...	12/2/2008 2:57:54...		Unacknowledged
<input type="checkbox"/>	Configuration Manager - Cont...	The user imports the data...	12/2/2008 2:56:41...		Unacknowledged
<input type="checkbox"/>	Data Security Manager - Adm...	Successful administrator l...	12/2/2008 2:57:54...		Unacknowledged
<input type="checkbox"/>	Data Security Manager - Dat...	Data fading occurred in fr...	12/2/2008 2:57:56...		Unacknowledged
<input type="checkbox"/>	Data Security Manager - Dat...	Data fading occurred in d...	12/2/2008 2:57:56...		Unacknowledged
<input type="checkbox"/>	Data Security Manager - Dec...	Decryption failed due to i...	12/2/2008 2:57:55...		Unacknowledged
<input type="checkbox"/>	Data Security Manager - Enc...	Encryption failed due to i...	12/2/2008 2:57:55...		Unacknowledged
<input type="checkbox"/>	Data Security Manager - Loc...	Lockdown occurred in fre...	12/2/2008 2:57:54...		Unacknowledged
<input type="checkbox"/>	Data Security Manager - Loc...	Lockdown occurred in dat...	12/2/2008 2:57:55...		Unacknowledged
<input type="checkbox"/>	Data Security Manager - Loc...	Lockdown occurred in dat...	12/2/2008 2:57:56...		Unacknowledged
<input type="checkbox"/>	Document Manager - Client di...	A file cannot be delivered...	12/2/2008 2:57:50...		Unacknowledged
<input type="checkbox"/>	Document Manager - Failed t...	Replication of a document...	12/2/2008 2:57:52...		Unacknowledged
<input type="checkbox"/>	Document Manager - Failed t...	Failed to export the data ...	12/2/2008 2:57:52...		Unacknowledged
<input type="checkbox"/>	Document Manager - Failed t...	Failed to import the data ...	12/2/2008 2:57:52...		Unacknowledged
<input type="checkbox"/>	Document Manager - No acc...	An administrator refreshe...	12/2/2008 2:54:45...		Unacknowledged


The Alerts page displays the following information about current alerts on your system:

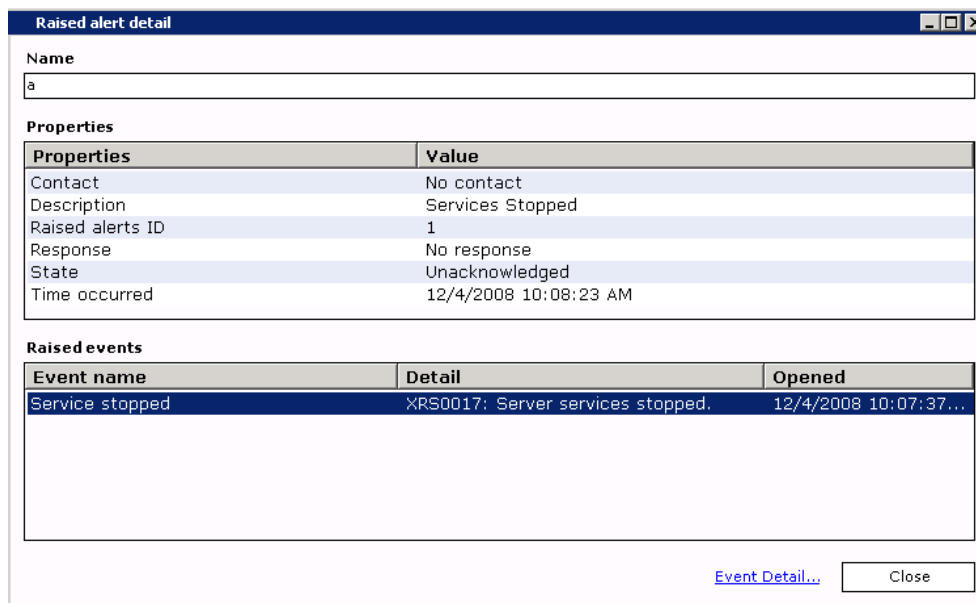
- **Raised alert** – Name of the alert; the alert is named when you define it.
- **Description** – A brief (optional) description of the alert provided when the alert was defined; it should contain relevant information for the parties responsible for viewing or responding to the alert.
- **Time opened** – Time the alert was raised on your system.
- **Time acknowledged** – Time the alert was acknowledged on your system.
- **State** – The current state of the alert: Unacknowledged, Acknowledged, or Closed.
- **Contact** – The contact information for this alert.

The icons that appear denote the alert priority:  *High*,  *Medium*, and  *Low*. You can sort information in each column by clicking the column headings, or you can rearrange the order of columns by clicking and dragging a column heading where you want it to be. To resize columns, grab the bar between headings and slide it to the right or left.

View alert details

The Raised alert detail window displays more information about the alert, as well as all of the events associated with it. You can access this window three ways:

- select an alert and click  **Raised alert detail**.
- double-click an alert.
- select an alert, right-click, and select **Alert detail** on the shortcut menu.



The Raised alert detail window appears and displays following information:

- **Name** – The name of the raised alert.
- **Properties** – This list box contains the following information about the alert:
 - *Contact* – The name of the contact assigned to this alert, if there is one.
 - *Description* – A description, if any, of the alert. This description is assigned when the alert is defined.
 - *Raised alert ID* – The numeric identifier your system has assigned to this alert.
 - *Response* – The type of response action associated with this alert, such as paging or e-mailing a person, or running an executable. When you acknowledge an alert, the response is stopped. For example, if you set the alert response to page someone, the system would no longer page that person once the alert was acknowledged.
 - *State* – The state of the alert, either Acknowledged or Unacknowledged.
 - *Time occurred* – The time the alert was raised.
 - *Contact* – The name for any contact assigned to this alert.
- **Raised events** – The Raised events list box displays the following information about all the events associated with the alert: Event name, Details, and the time the events that triggered the alert occurred. You can view the details about each event in this list box by selecting it and clicking **Event details**.



Because some of the events that trigger alerts may occur on client devices, some alerts may not appear immediately after they occur. Events that occur on a client device are sent only when clients connect to the server.

The Raised event detail window appears and displays the following fields:

Event. The name of the raised event.

Properties. This list box contains the following information about the event:

- *Description* – A brief description of the event.
- *Machine* – The name of the computer on which the event occurred.
- *Raised event ID* – The numeric identifier assigned to this event.
- *Time occurred* – The time the event occurred on a particular computer. If the computer is in another time zone, the Time Occurred field will reflect the time the event occurred in the time zone where the event originated.
- *Time opened* – The time that the alert was raised by the triggered event.

The screenshot shows a window titled "Raised event detail" with the following content:

Event
Service stopped

Properties

Property	Value
Description	Successful Service Shutdown
Machine	AFARIAW2K3R2
Raised event	14
Time occurred	12/4/2008 10:07:37 AM
Time opened	12/4/2008 10:07:37 AM

Details
XRS0017: Server services stopped.

Close

Details – Any other pertinent details about the event.

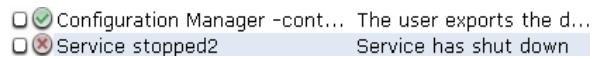



Any message that appears in the Raised event detail dialog box has a maximum of 255 characters. To view the entire message, see the All raised events view in Data views, Logs.

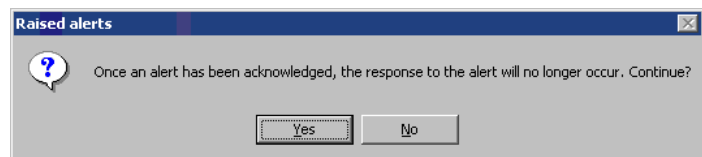
Acknowledge an alert

Once you, your system administrator, or a designated contact has been notified that an alert has been raised on your server, you should acknowledge the alert as soon as possible. When you acknowledge an alert, you do not close the alert. You simply let other people who work with the server know that someone knows about the alert and is taking steps to resolve whatever problem might have occurred. Acknowledging the alert will stop any response that was defined for the alert, such as paging or sending e-mail to a contact.

To acknowledge an alert, in the Alerts area, you select the check box next to the raised alert you want to acknowledge.




You can also select an alert and click  **Acknowledge alert(s)** on the toolbar, or right-click and select **Acknowledge** on the shortcut menu. A message box appears asking if you want to continue.



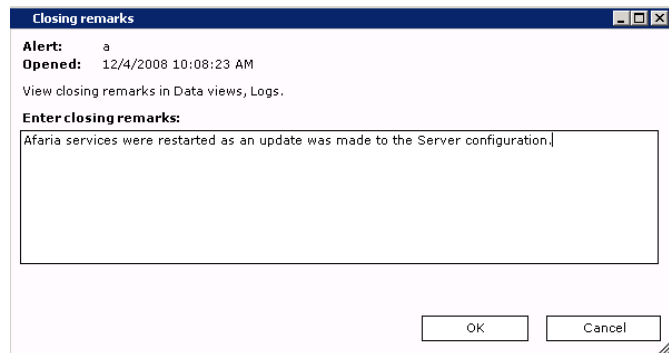
You can click **Yes** to acknowledge the alert, or click **No** if you want the alert response to continue. Notice in the main window that the state of the alert changes from Unacknowledged to Acknowledged.

Close an alert


When you close an alert, use the Closing remarks dialog box to add any comments, such as what the exact problem was and how it was handled. You can view any closing remarks you enter here through Data views, Logs.

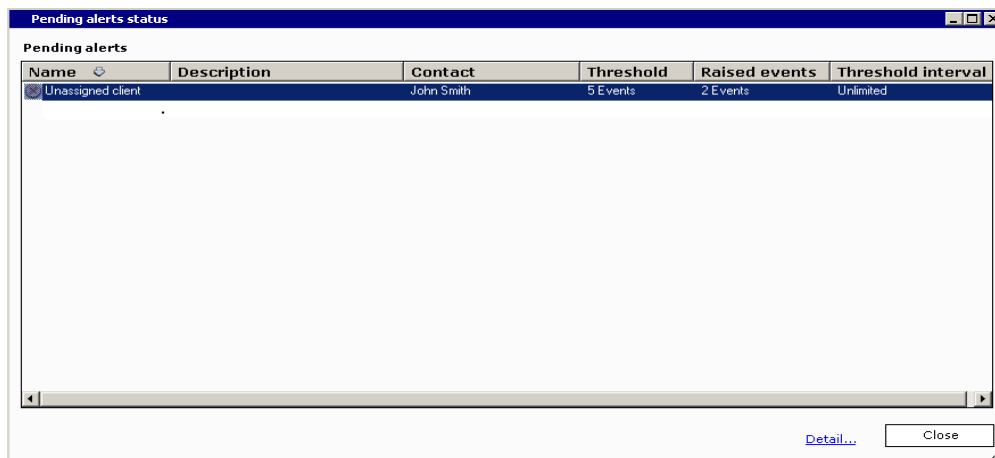
To close an alert, in the Alerts area, you highlight the alert you want to close and click  **Close alert(s)** on the toolbar, or right-click and select **Close** on the shortcut menu. The Closing remarks dialog box appears.

You can enter any comments you have about the alert in the Closing remarks area, but this is not required. You click **OK** to close the alert. The alert is removed from the Alerts list.



View pending alerts

Pending alerts are alerts for which *at least one* event supposed to trigger the alert has occurred. You click  **Pending alert status** on the toolbar to display the Pending alert status window.

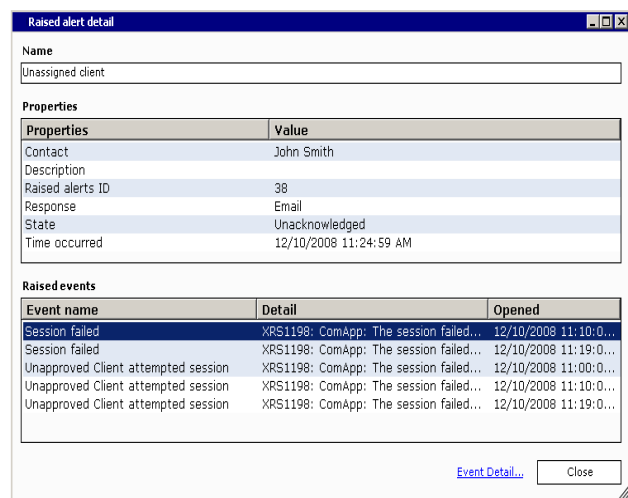


The Pending alerts window displays the following information:

- **Name** – Name of the pending alert.
- **Description** – Description of the pending alert; this description is entered when the alert is defined.
- **Contact** – Name of contact associated with this alert, if any.
- **Threshold** – The number of events that must be triggered in order for the alert to be raised.
- **Raised events** – The number of raised events that have already been triggered.
- **Threshold interval** – The time period during which the events must be triggered in order for the alert to be raised; for example, there must be three events triggered within an hour for the alert to be raised.

To view the details of a pending alert, click **Details**. The Pending alert details dialog box appears and displays the following information:

- **Pending alert** – Name of the pending alert.
- **Properties** – This area contains the following fields:
 - *Interval* – The time interval during which events must be triggered.
 - *Priority* – The priority of the alert: Low, Medium or High. This is determined when the alert is created.
 - *Raised events* – The number of events that have triggered.



- *Status* – The status of the alert: Enabled or Disabled.
- *Threshold* – The number of events that must be triggered in order to raise the alert.
- **Raised events** – This list box contains the following fields:
 - *Name* – The name of the triggered event.
 - *Detail* – A description of the triggered event.
 - *Opened* – The time the event was triggered.

You can select an event in the list and click **Event detail** to view more information about the event. The Raised event detail window appears. For more information about the fields in this window, see [“View alert details” on page 73](#).

Reports

Home > Reports

The Reports page lets you access key system and activity data stored in the server database schema. You can also develop your own custom reports, which appear in the list alongside the predefined reports listed on the Reports page. To access Reports, click **Home > Reports**.



Running reports

- 1 Generate reports by right-clicking the report and selecting **Open this report**.
- 2 Depending on the report you choose, an additional dialog box may open to prompt you for criteria such as a date range.
- 3 Click **Run**.

The report opens in the Crystal Reports Viewer.

The first view you see is the Main Report page. Many reports contain all of the report information on the Main Report page.

About report results

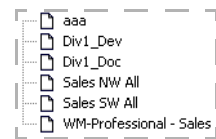
Consider the following items about report results:

- Data from clients – reports that contain data as reported by clients are current up to the most recent client connection.
- Handheld Client Security and Windows Client Security reports – the date range for the reports reflects the date the client connected to the server so that the action could be reported, rather than when the action happened.
- Inventory report Windows Software by Client – phone and network data collected and reported by Inventory Manager varies by device type. See “Collecting phone and network data on handhelds” located in the *Afaria Reference Manual | Components*.

- License Compliance reports:
 - Report Client Usage Detail – if you run this report and receive a message that no data exists, run a new inventory scan on your clients and then re-run the report.
 - Report Installations Below Threshold – reports that require license allocations are compiled by allocating the licenses with the longest expiration horizon first and then allocating licenses with shorter horizons.

About reports with navigation

Some reports generate a navigation pane that includes bookmarks to make it easier for you to locate specific information within the report. For example, if you run the Client Groups report, when the report has generated you will see a navigation pane on the left.



Click on a bookmark to navigate to the bookmark in the report.

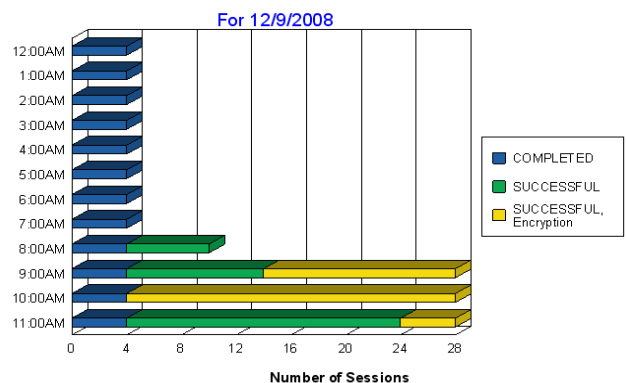
If you select BlackBerry in the left pane, the area in the report is highlighted, making it easier for you to locate information about that client group:

Group name	Sales NW All	Group type	Static
Client name		Client type	
ENGWIN2K3VM		Windows	

About reports with graphical information

Additionally, some reports will display the information in a graph or pie chart on the main report window. You can click on an area of the graph or pie chart to display more detailed information.

For example, if you run the Session Hourly Summary report, when the report has generated you will see a graph that looks like the one to the right:



If you hover the cursor over the chart, you see a magnifying glass. If you double-click on an area, a new tab appears and displays detailed information. For example, if you double-click on Successful sessions at 7:00 PM, a new tab appears that lists the details of each successful session during the 7:00 hour.

Session Log

12/9/2008 12:42:53PM

AFARIAW2K3R2					SUCCESSFUL	
Date	Start time	End time	Duration	Client name	Client type	
12/9/2008	8:48:55AM	8:49:17AM	00:00:22	WIN_XP1234	Windows	
12/9/2008	8:49:04AM	8:49:10AM	00:00:06	AFARIAW2K3R2	Windows	
12/9/2008	8:53:55AM	8:54:26AM	00:00:31	WIN_XP1234	Windows	
12/9/2008	8:54:03AM	8:54:09AM	00:00:06	AFARIAW2K3R2	Windows	
12/9/2008	8:58:55AM	8:59:20AM	00:00:25	WIN_XP1234	Windows	
12/9/2008	8:59:03AM	8:59:09AM	00:00:06	AFARIAW2K3R2	Windows	

Total Sessions : 6
Total Duration : 00:01:36

To return to the graph, you can click the **Main Report** tab, or you can click the **Close current view** icon on the toolbar. To view the details for another item, you simply double-click on another area of the graph.

About tenants and reports

Support – Multitenancy

In a multitenant environment, some reports are filtered by your current tenant context and some reports are not. You can run reports to review operational data from your database that is not filtered by tenant. For example, you may be interested in reviewing the number and nature of file transfers, for all tenants, in a single report. Many other reports are filtered to run only for a single tenant, based on your current tenant context.

About Creating custom reports

You can generate custom reports using Visual Studio .NET or Crystal Reports. To view custom reports via the Administrator Reports window, you must copy the reports you create to the VafariaReports folder located under the directory where you installed the Afaria Administrator.



You must close the Afaria Administrator interface prior to creating any new folders, then restart the Administrator to continue.

You need three major components in order to create a functioning custom report that you can view from the Afaria Reports window:

- **An XML schema definition (XSD) file** – The XSD file represents a set of data. It defines the name and data types for the fields displayed in the report.
- **A Crystal Report with the components of the XSD file placed on the report** – When you design a report, the XSD file is pointed to as the data source. Because this is a data format rather than a hard-data location, the report does not have to be re-bound to other data

sources as it is distributed. The fields in the XSD file can be added to the report through Visual Studio .NET.



You can create custom reports in Crystal Reports without the XSD file; however, the report will not function or appear in the same format as Afaria's pre-defined reports.

- **An accompanying Report Information File (RIF)** – The RIF tells Afaria which data to extract from the database in order to place it in the report. Two components of the RIF facilitate this process: a database query and parameters.
 - *Database query.* The output of the queries must exactly match the format described in the XSD file. Afaria looks for an RIF with the same name as the report in the \AfariaReports folder and executes the query against the database using the credentials defined during the Afaria Server installation.
 - *Parameters.* Along with the database queries, the RIF defines any parameter fields used to narrow the amount of data the query returns. For example, when you run a report, you can enter a date range and insert it into the database query.

Afaria supports four parameter types: Text, Date, DateTime, and Combo. You can also use a <DefaultValue> tag to automatically fill in the parameter value at report runtime.



If you use the keyword [All] in the <DefaultValue> tag, Afaria replaces it with an asterisk (*) at runtime.

The Combo type parameter field contains the <DisplayMember> and <ValueMember> tags. The database query uses the property within the <ValueMember> tag, and the parameter field dialog box uses the <DisplayMember> tag. Use the <SQL> tag to specify the SQL statement that returns the values to populate the combo box. If there is only one value for the combo box, Afaria bypasses the parameter field prompt when you launch the report.

Custom reports and your multitenancy environment

Support – Multitenancy

The multitenancy database design has implications for custom reports. The system attempts to filter custom results by tenant by modifying the associated SQL script at runtime. However, it may not always be successful. Therefore, test your custom items after accumulating data for multiple tenants to evaluate how they are 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 with modifications. Generally, adding a tenant-specific property allows the system to filter by tenant.

Custom items that you create are available to all tenants, rather than only for the originating tenant.

Creating custom reports

To generate the same format as Afaria pre-defined reports, you should use VisualStudio .NET to create your custom reports. You can also build custom reports in Crystal Reports, but they do not follow the Afaria format.

- 1 In VisualStudio .NET (VS.NET), add a new XML Schema file to the current project. Enter a report name. This file will have the .xsd extension.
- 2 Ensure you have selected the Schema view and that the VS.NET Toolbox is showing.
- 3 Drag an element from the Toolbox onto the Schema view and name it Qry. Afaria requires that you name this element Qry.
- 4 Under Qry, add an element named ClientName. You will see an "E" to the left. Ensure it is a string value. If it isn't, right-click on the box to display a drop-down list of datatypes.
- 5 Add a new report to the project. This file will have the .rpt extension.
- 6 Select Using the Report Expert.
- 7 On the Data tab, select More Data sources, ADO .NET. The XML file path will be the path to the .xsd you created earlier.
- 8 On the Data tab, insert the Qry table.
- 9 On the Fields tab, add the qry.ClientName field.
- 10 On the Style tab, enter a Title for the report. At this point, the report is complete, and you must tell Afaria how to populate the data into the XSD format using the RIF.
- 11 Add a new XML file to the project.
- 12 Save the XML file with the same name as the report file. This file will have the .xml extension.
- 13 You must have the following tags for the RIF: <Report>, <Name>, <Description>, and <SQLString> or <OracleString>. Use <Parameter> tags if you plan to use parameters. An example:

```
<?xml version="1.0" encoding="utf-8" ?>
  <Report>
    <Name>Client List<\Name>
    <Description>This report displays a list of Clients.<\Description>
    <SQLString>
```

```
SELECT Clientname  
FROM dbo.A_Client
```

<\SQLString>

<Parameters>

<\Parameters>

<\Report>

- 14 Copy the .rpt and the .xml files into the \AfariaReports folder on the computer where the Afaria Administrator is installed.
- 15 Rename the .xml file to .rif. For example, you would rename Simple.xml as Simple.rif.
- 16 In the Afaria Administrator, click **Home > Reports**. The Reports window opens and displays the report you created.

Client deployment

After creating Afaria Client installation packages for each type of client device you need, you must deploy the packages to each client. Use the Client Deployment area of your Afaria solution to support your use of the Afaria OTA Deployment Center to deploy Afaria Clients to devices. See [“Sending notifications” on page 101](#) for instructions on sending notification messages to end users. See [“OTA Deployment Center” on page 142](#) for configuring the deployment center for operations.

To view the Client Deployment page, click **Home** on the global navigation bar and select **Client Deployment**. The Client Deployment page appears.

From the left navigation pane you can work with the following tools:

Home > Client Deployment

- **Address Book** – Use the Address Book links to manage client addresses and distribution lists for deployment notifications, as well as to send client notifications. See [“Address book properties” on page 87](#) and [“Sending notifications” on page 101](#).
- **Notification Messages** – Use the Notification Messages links to manage templates related to client notifications, as well as to send client notifications. See [“Notification templates” on page 91](#) and [“Sending notifications” on page 101](#).
- **Self-service Portal** – Use the Self-service Portal links to access tools used to support your custom-developed, self-service portal, as well as to manage network access points used for client deployment. See [“Self-service portal settings” on page 108](#).

Address Book
Addresses
Distribution Lists
Notification Messages
Message Templates
OMA CP Templates
Free-form Templates
Self-service Portal
Access Points
Supported Device Types
Supported Platforms








Client deployment toolbar

The Client Deployment toolbar is always available to you and contains both buttons and menus.

Home > Client Deployment



Use the toolbar to access the following commands.

<i>Toolbar icon</i>	<i>Name</i>	<i>Description</i>
	<i>New</i>	Creates a new item of the type selected from the button's submenu. After selecting the type of item you wish to create, complete the item's properties and save it.
	<i>Edit</i>	Accesses the properties for the item you currently have selected, after which you can make and submit changes to the item.
	<i>Copy</i>	Creates a copy of the item you currently have selected, after which you can make and submit changes for the new item.
	<i>Delete</i>	Removes the item you currently have selected. Prior to removal, the system displays a dialog box requesting confirmation of the item's deletion.
	<i>Refresh</i>	Reloads all data items for the page you currently have displayed. Any changes made to items since the system last displayed the page will be shown in the refreshed display.
	<i>Send Message</i>	Opens the Send Notification Message dialog box for the type of notification selected on the button's submenu. After selecting the type of notification you wish to send, complete the notification's properties and send it. See "Sending notifications" on page 101 .
	<i>Import Addresses</i>	Opens the Address List dialog box, which lets you import into your address book a Comma-Separate Values (CSV) file containing client and device addresses. See "Importing addresses" on page 89 .

Address book properties

The address book lets you maintain addresses and distribution lists used for OTA Deployment Center notifications. You can enter each device address individually, or import addresses from a file in standard CSV format.

Home > Client Deployment > Addresses

FirstNa...	Last Name	Address
Bert	Thomas	6567171117@r
Charlie	Brown	4145698989@r
Dan	Walker	8189596659@r
Joe	James	3135256565@r
John	Doe	3154547474@r

Use the address book to hold all addresses related to client deployment. Addresses may be in the form of an e-mail address or an SMS address. You can also organize addresses into distribution lists; see [“Distribution list properties” on page 88](#).

After adding an address, you can edit, copy, or remove the address entry, as well as send a notification to one or more addresses. Each address has following properties.

Home > Client Deployment > Addresses > Edit Address

The screenshot shows a dialog box titled "Edit Address" with a close button (X) in the top right corner. It contains the following fields and controls:

- Address:** A text input field containing "14445882323@mycom.com". To its right is a "Save" button.
- First Name:** A text input field containing "Charles". To its right is a "Cancel" button.
- Last Name:** A text input field containing "Brown".
- Description:** A text area containing "work/sync email".

- **Address** – Provide a valid e-mail or mobile number to which Afaria sends notifications. See [“Addresses and routing for Afaria messages” on page 150](#) to learn about how address formats affect notification routing.
- **First Name** – Provide the first name for the notification recipient.
- **Last Name** – Provide the last name for the notification recipient.
- **Description** – Provide any additional descriptive text that helps to identify the recipient.

Distribution list properties

Use distribution lists to organize your client deployment addresses into groups. After organizing addresses into distribution lists, you can send notifications to all addresses in the list. In addition, you can import addresses into a distribution list from a standard CSV file.

Home > Client Deployment > Distribution Lists

Distribution Lists	
Name	Description
All Afaria Clients	General list of all client type users
Blackberry	All users who use Blackberry dev..
Palm Devices	List of all users that used Palm d...
Symbian os 9x device	All users that use the 9x devices
Windows Mobile Profess...	All users that use WM Profession...

After creating a distribution list, you can edit, copy, or remove the list. Each distribution list in your address book has following properties.

Home > Client Deployment > Distribution Lists > Edit Distribution List

Edit DistributionList

Name:

Description:

Available Addresses

First N...	Last Name	Address
Joe	James	3135256565@...
Richard	Gill	5552811234@...
Sue	Sanders	5744443844@...

Addresses

First Na...	Last Na
Bert	Thomas
Charlie	Brown
Dan	Walker
John	Doe
John	Smith

- **Name** – Provide a descriptive name to identify the distribution list.
- **Description** – Provide any additional descriptive text that helps to identify the list.
- **Available Addresses** – Contains all addresses not currently assigned to the list.
- **Addresses in List** – Contains all addresses currently assigned to the list.

Importing addresses



- 1 To import addresses, click the **Import Addresses** icon on the toolbar.

To import addresses into a distribution list, click the **Import** button on the Edit Distribution List window.

The Address List dialog box displays.

- 2 Navigate to the CSV file you want to import, and then click **Open**. See [“Formatting a CSV file of addresses” on page 90](#) to learn more.

The system validates the contents of the CSV file and then displays the Import Addresses window.

Home > Client Deployment > Distribution Lists > Import Addresses

Import Addresses

Invalid Addresses

Status	Address	First Name	Last Name
INVALID	(675) 443-1234	James	Burgess
INVALID	543	Bob	Brown
DUP_IMPORT	66634331234...	Dennis	Newman
DUP_IMPORT	66634331234...	Tom	Baker
DUP_IMPORT	6665431234@...	Baker	
DUP_IMPORT	6665431234@...		

Valid Addresses Available to Import

Address	First Name	Last Name
2835431234@my...	Doug	Baker
33543341234@m...		
6643431234@my...		

Valid Addresses Selected to Import

Address	First Name	Last Name
3423431234@m...	Kim	Sanc
63434431234@...	Tim	Brow
6344431234@m...	Harry	Ford
3435431234@m...	James	Sanc

➤

↔

⬅

⏪

Invalid Addresses – Contains improperly formatted addresses or duplicated addresses. double-click an entry in the list to make corrections to the entry.

Valid Addresses Available to Import – Contains valid entries from the CSV file that are eligible for import.

- 3 Use the arrows to move addresses between the lists.
- 4 To import the addresses you have selected, click **OK**. The total number of addresses imported displays in the Addresses Imported dialog box.
- 5 Click **OK**.

If you have imported addresses into a distribution list, all imported addresses are automatically added to the distribution. You can make any additional changes to the distribution list that you require. See [“Distribution list properties” on page 88](#).

Formatting a CSV file of addresses

To import a CSV file of addresses into your address book, ensure you observe the following rules for your CSV file. If you do not observe these rules, your import may not work or the results of your import may require significant editing.

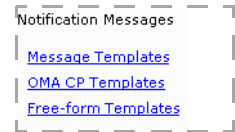
<i>Rule</i>	<i>Description</i>	<i>Notes</i>
Delimiter	Comma	Every field value, except the last field in a row, must be followed by the delimiter. For example: john@mydomain.com,John,Doe,John's description 8725551212,Jane,Doe,Jane's description
End-of-line character	CR/LF, CR, or LF	
Field order	Address, First Name, Last Name, Description	
Required fields	Address	
Optional fields	First Name, Last Name, Description	Use consecutive delimiters to indicate omitted field values, e.g.,: johndoe@mydomain.com,,, 5725551212,,,
Header row	None	A header row will be rejected as an invalid address.

Notification templates

Use notification templates to build reusable notifications. Client Deployment provides you with different types of notification templates.

Home > Client Deployment

- **Message Templates** – Use for OTA notifications. See [“Message template properties” on page 92](#).
- **OMA CP Templates** – Use for OMA CP notifications. See [“OMA CP template properties” on page 93](#).
- **Free-form Templates** – Use for custom, Wireless Application Protocol (WAP) provisioning documents, e.g., OMA CP notifications, as well as for any other type of messages. See [“Free-form template properties” on page 99](#).



Message template properties

Message templates are designed to work in conjunction with your OTA Deployment Center. The message template contains information provided to device holders that instructs them to visit the deployment center's Web site to download the client. See ["OTA Deployment Center" on page 142](#) to learn more.

Message Templates		
Template Name	Description	Subject
Afaria client deploym...	Standard notification for u...	Update your Af
Notifications for exec...	Standard notification sent ...	Afaria client up
Test template	Used by IT for testing	Afaria update

Each Message template contains the following properties.

Home > Client Deployment > Message Templates

Edit Message Template

Name: Afaria client deployment notification

Description: Standard notification for updated Afaria clients

Subject: Update your Afaria Client

Message: <RecipientName>
<URL-Pkg-1>

- **Name** – A unique name for the template.
- **Description** – An optional description for the template.
- **Subject** – The subject line for all notifications based on the template.

- **Message** – The body text included in the notification. At least one package URL is required for this field.



SMS messages sent via SMTP cannot exceed 160 characters. If the **Message** field exceeds 160 characters, you will see a warning when saving your template that advises you of a potential problem sending the message.

- If you are sending via an SMS Gateway, you can proceed. See “[SMS Gateway](#)” on page 144 to learn more.
- If you are sending via SMTP, consider editing the message so the sum of all characters from the message as well as values substituted for variables will not exceed 160 characters.

To insert one or more variables in the body, click in the **Message** field where you want the variable’s value to display, and then use the variable links provided.

- **Insert Package URL** – Adds a substitution variable to the template, which becomes a URL from which the recipient downloads an installation package from the OTA Deployment Center. To include multiple packages in a notification, add multiple package URL variables and then edit each variable name to be unique, e.g., “<URL-pkg-1>”, “<URL-pkg-2>”, etc. The actual package URLs used are selected at the time the notification is sent. At least one package URL is required.
- **Insert Recipient Name** – Adds a substitution variable to the template, which becomes a recipient’s first and last name. Due to the potential number of characters added to the notification, avoid using this variable for SMTP-based SMS messages. The name used is based on the recipient list defined for the notification when sending occurs.
- **Insert First Name** – Adds a substitution variable to the template, which becomes a recipient’s first name. The name used is based on the recipient list defined for the notification when sending occurs.
- **Insert Last Name** – Adds a substitution variable to the template, which becomes a recipient’s last name. The name used is based on the recipient list defined for the notification when sending occurs.

OMA CP template properties

OMA CP templates are used to send device notifications formatted according to the OMA CP standard. When received by the device, the notification provisions it with settings to enable communication. After provisioning, the device holder may need to set the device’s default access point to the access point created by OMA CP before visiting the Web-based OTA Deployment Center. From the OTA Deployment Center the device holder can install the Afaria Client. Provisioning is required for a new device or for a device that has undergone a hard reset.



- OMA CP is a device-independent standard for provisioning mobile devices. It is the administrator’s responsibility to evaluate devices to determine whether or not they support the OMA CP standard.
- OMA CP notifications are always sent via the Afaria SMS Gateway.

Home > Client Deployment > OMA CP Templates

OMA CP Templates	
Template Name	Description
GPRS 1245	Building 1245 GPRS settings
GPRS NW Sales	NW Sales GPRS Settings
GPRS VoxWire	VoxWire GPRS Settings

Since notifications sent using OMA CP contain provisioning settings, little or no interaction is required from the device holder. After the device receives the OMA CP notification, the device holder can use the new settings to access the network and the OTA Deployment Center.

How OMA CP provisions a device

See the following overview to learn about how provisioning through OMA CP functions to establish a device as an Afaria Client.

Provisioning step	Device state
1. Device holder receives a new device, experiences a hard reset, or has otherwise lost network connectivity.	Unprovisioned
2. Afaria administrator creates OMA CP notification for provisioning. Afaria administrator embeds home page URL for downloading the installation package from the OTA Deployment Center. ^{a,b}	Unprovisioned
3. Afaria administrator sends OMA CP notification to the device.	<ul style="list-style-type: none"> Provisioned Browser configured to display the package URL when next opened^a
4. Device holder sets default access point on device to the access point created by OMA CP.	Provisioned and ready for network access.
5. Device holder launches Web browser.	OTA Deployment Center accessed automatically ^a
6. Device holder downloads and launches the Afaria installation package for the device.	Afaria Client installed
7. Afaria Client contacts Afaria Server for its first session.	Afaria Client established

a. Embedding the package URL is optional.

b. A Message template or Free-form template can also be used to notify users to visit the OTA Deployment Center.

Device differences for OMA CP at the client

The end-user experience when a device receives an OMA CP notification may differ significantly from device to device. It is important that you test each type of device you plan to provision, and then provide end users with any additional information necessary for provisioning success.

Device-based differences users may experience include:

- A device user may need to open the OMA CP notification for provisioning to occur.
- The OMA CP notification may trigger a security prompt before provisioning changes occur.
- An OMA CP notification may remain in the end user's Inbox.
- A device may ignore some provisioning settings in the notification.
- A device may block the OMA CP notification for security reasons.

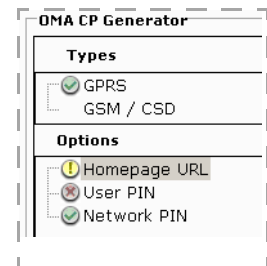
A device user may need to set the device's default access point to the one added by OMA CP.





OMA CP template validation

In addition to basic template properties, you can access additional template properties through the list displayed in the OMA CP Generator pane.

Home > Client Deployment > OMA CP Templates

The current validation status for each property group displays in the left pane. Although you can save a template with invalid properties, you should correct any errors prior to sending a notification based on the template.



<i>Status icon</i>	<i>Description</i>
Blank	Property omitted from template.
	Property included in template and has passed validation.
	Property included in template but has not yet been validated. To validate a property, click the Validate button.
	Property included in template, but is invalid. Correct the property value found in the right pane. To re-validate, click the Validate button.
	An invalid property in the right pane displays with the attention icon.

Basic properties

Basic properties provide general information to identify the template, as well as command buttons for performing template-related tasks.

Home > Client Deployment > OMA CP Templates



The screenshot shows a form with two text input fields and four buttons. The first field is labeled 'Name:' and contains the text 'allcellular GPRS'. The second field is labeled 'Description:' and contains the text 'My Cellular's GPRS Settings'. To the right of the fields are four buttons: 'Save', 'Cancel', 'Validate', and 'Show XML'.

- **Name** – A unique name for the template.



The OMA CP template name will be the name of the access point configured on the device.

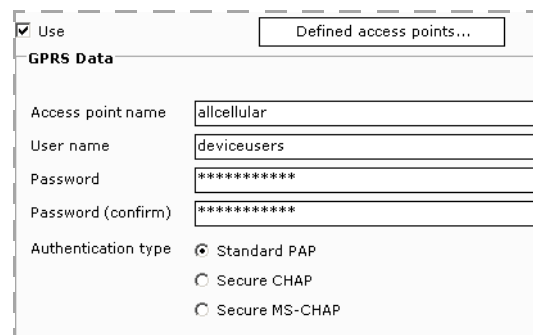
- **Description** – An optional description for the template.
- **Save** – Stores all template settings.
- **Cancel** – Discards all changes made to template settings.
- **Validate** – Checks all template settings and identifies any invalid properties.
- **Show XML \ Show Form** – Toggle the display between form view and XML view. The XML view enables copy and paste commands.

Network service types – GPRS properties

GPRS properties provide access to a General Packet Radio Service (GPRS) network. Use of a GPRS network in the template precludes the use of a GSM / CSD network.

Home > Client Deployment > OMA CP Templates > Types > GPRS

- **Use in template** – Select to use the items on the page as the properties enabled by default when sending a notification. Regardless of the check box's status (selected or cleared), all properties on the page are saved with the template.
- **Defined access points** – Select to apply a predefined GPRS access point definition to the template. After applying a predefined access point you can modify the settings. For more about predefined access points, see ["Access point properties" on page 108](#).



The screenshot shows a form titled 'GPRS Data' with a 'Use' checkbox checked. There is a button labeled 'Defined access points...'. Below are several input fields: 'Access point name' (allcellular), 'User name' (deviceusers), 'Password' (masked with asterisks), and 'Password (confirm)' (masked with asterisks). At the bottom, there are three radio buttons for 'Authentication type': 'Standard PAP' (selected), 'Secure CHAP', and 'Secure MS-CHAP'.

The remaining data values are defined by your GPRS service provider, which may not require all available fields.

Network service types – GSM / CSD properties

GSM / CSD properties provide access to a Global System for Mobile communications (GSM) / Circuit Switched Data (CSD) network. Use of a GSM / CSD network in the template precludes the use of a GPRS network.

Home > Client Deployment > OMA CP Templates > Types > GSM / CSD

- **Use in template** – Select to use the items on the page as the properties enabled by default when sending a notification. Regardless of the check box's status (selected or cleared), all properties on the page are saved with the template.
- **Defined access points** – Select to apply a predefined GSM / CSD access point definition to the template. After applying a predefined access point you can modify the settings. For more about predefined access points, see [“Access point properties”](#) on page 108.

The remaining data values are defined by your GSM / CSD service provider, which may not require all available fields.

Options – Home page URL properties

The home page URL is embedded into the template and can be either the package URL variable or a hard-coded URL of your choosing. Using this feature can avoid the need to send out an OTA Deployment Center notification subsequent to provisioning. When the client user launches the device browser after receiving the notification, the browser is directed automatically to the URL defined by this field. Use of the home page URL is optional for an OMA CP notification.



Not all devices react the same way to the use of Options settings. Be sure to test the effect on devices for the Options properties you plan to use.

Home > Client Deployment > OMA CP Templates > Options > Homepage URL

- **Use in template** – Select to use the page properties as those enabled by default when sending a notification. Regardless of the check box's status (selected or cleared), all properties on the page are saved with the template.
- **Insert Package URL** – Adds a substitution variable to the template, which becomes the URL from which the recipient downloads an installation package.
- **Home page URL** – Click this field, and then click the **Insert Package URL** button to add the package URL substitution variable to the template. You may also enter a hard-coded URL to

store in the template. If the package URL variable is used, a package is selected at the time the notification is sent. Use of multiple package URLs is not supported for OMA CP.

Options – User PIN properties

Use of the User PIN is optional for an OMA CP notification.



Not all devices react the same way to the use of Options settings. Be sure to test the effect on devices for the Options properties you plan to use.

Home > Client Deployment > OMA CP Templates > Options > User PIN

- **Use in template** – Select to use the page properties as those enabled by default when sending a notification. Regardless of the check box's status (selected or cleared), all properties on the page are saved with the template.
- **User PIN** – Enter a numeric authentication code provided to allow the device to accept the notification. A single user PIN can be used for multiple devices.

The screenshot shows a configuration form for OMA User Pin Information. At the top, there is a checked checkbox labeled "Use in template". Below this, the section is titled "OTA User Pin Information". There is a text input field labeled "User PIN" containing the value "58958".

Options – Network PIN properties



Not all devices react the same way to the use of Options settings. Be sure to test the effect on devices for the Options properties you plan to use.

Use of the Network PIN is optional for an OMA CP notification.

Home > Client Deployment > OMA CP Templates > Options > Network PIN

- **Use in template** – Select to use the page properties as those enabled by default when sending a notification. Regardless of the check box's status (selected or cleared), all properties on the page are saved with the template.
- **Network PIN**. Enter a numeric authentication code provided to allow the device to accept the notification. A device may require a network PIN to accept an OMA CP notification. The network PIN should specify the International Mobile Subscriber Identify (IMSI) for the recipient's Subscriber Identify Module (SIM) card. For this reason, a network PIN is valid only for a single mobile number.

The screenshot shows a configuration form for OMA Network Pin Information. At the top, there is a checked checkbox labeled "Use in template". Below this, the section is titled "OTA Network Pin Information". There is a text input field labeled "Network PIN" containing the value "23242".

Free-form template properties

Free-form templates are used to send devices custom, WAP provisioning documents, e.g., OMA CP notifications, as well as for any other type of messages. If you are using the free-form template to create OMA CP messages, you can also include the User PIN and Network PIN. For any free-form message you can include a package URL.

Home > Client Deployment > Free-form Templates

Free-form Templates	
Template Name	Description
Buldg 1245 GPRS	Building 1245 GPRS settings
GPRS VoxWire	VoxWire GPRS Settings
SalesNW GPRS	NW Sales GPRS Settings



Caution advisory!

Although validation is provided for the structure of an XML document when sending a message based on a free-form template, the system cannot determine the effect the message will have on a device. It is the administrator's responsibility to provide meaningful and accurate settings. Prior to deploying the notification, test it with the type of device that will receive the notification.



- OMA CP is a device-independent standard for provisioning. It is the administrator's responsibility to evaluate devices to determine whether or not they support the OMA CP standard.
- Free-form notifications are always sent via the Afaria SMS Gateway.

Each Free-form template contains the following properties.

Home > Client Deployment > Free-form Templates

Edit Free-form Template

Name:

Description:

Body:

- **Name** – A unique name for the template.

- **Description** – An optional description for the template.
- **Body** – The free-form text included in the SMS notification. A package URL is optional for this field. The body can be XML or a text message.
- **Save** – Stores all template settings.
- **Cancel** – Discards all changes made to template settings.
- **Include User PIN** – When using the free-form template to create your own OMA-CP-compliant notification, you can select to add a User PIN to the template. Including the User PIN enables entry of a numeric authentication code provided to allow the device to accept the message. A single user PIN can be used for multiple devices.
- **Include Network PIN** – When using the free-form template for an OMA CP message, you can select to add a Network PIN to the template. Including the Network PIN allows the device to accept the message. A device may require a network PIN to accept an OMA CP notification. The network PIN should specify the International Mobile Subscriber Identify (IMSI) for the recipient's Subscriber Identify Module (SIM) card. For this reason, a network PIN is valid only for a single mobile number.



Only OMA-CP-compliant messages will utilize User and Network PINs.

- **Insert Package URL** – Adds a substitution variable to the template, which becomes a URL from which the recipient downloads an installation package. To include multiple packages in a notification, add multiple package URL variables and then edit each variable name to be unique, e.g., "<URL-pkg-1>", "<URL-pkg-2>", etc. The actual package URLs used are selected at the time the notification is sent.

Sending notifications

Use the Send Notification feature to generate and deliver notification to one or more devices. You can send the following types of notifications:

- Message notifications – Tell device holders about the publication of new Afaria Client installation packages on the OTA Deployment Center. Afaria routes message notifications to recipients via the SMS gateway or your SMTP server.
- OMA CP notifications – Send notifications to provision devices for access to the OTA Deployment Center, and optionally provide automatic navigation to the installation package URL. Afaria routes OMA CP notifications to mobile devices via the SMS gateway.
- Free-form notifications – Send custom, WAP provisioning documents, e.g., OMA CP notifications, as well as for any other type of messages. Afaria routes free-form notifications to mobile devices via the SMS gateway.

See [“About notification delivery” on page 107](#) to learn more about message routing.

Prerequisites for sending notifications

Before you can send notifications to devices, you must:

- Configure the mechanism for sending message notifications.
 - See [“SMTP” on page 158](#) to learn about configuring an SMTP server.
 - See [“SMS Gateway” on page 144](#) to learn about configuring an SMS gateway.
- Configure access to the OTA Deployment Center download interface settings used when sending notifications to clients and defining Web services interface settings for the OTA Publisher. See [“OTA Deployment Center” on page 142](#) for information on configuring the deployment center.
- Publish client installation packages to the OTA Deployment Center.

Sending notifications based on addresses or distribution lists

- 1 Select **Addresses** or **Distribution Lists** in the left pane of the Client Deployment page. The right pane lists all items corresponding to the type you selected.
- 2 Click the **Send** icon on the toolbar, and then select the type of notification you wish to send.



You can also pre-select recipients by choosing one or more items in the right pane, right-clicking, and choosing **Send** from the shortcut menu.

The Send Notification Message window displays. If you have selected any recipients, the **To** field populates automatically with the associated addresses.

Home > Client Deployment > Addresses > Send Message > Message Notification

Send Notification Message

Template: Afaria client deployment notification

Batch Name: Afaria client deployment notification

Batch Description: Standard notification for updated Afaria clients

To: {Windows Mobile Professional}

Subject: Update your Afaria Client

Message: <RecipientName>
<URL-Pkg-1>

Message Variables

- Insert Package URL
- Insert Recipient Name
- Insert First Name
- Insert Last Name

Send

Cancel

Validate

Message notification example

3 To generate a notification message based on a predefined template, use the **Template** drop-down list to select a template. Notification fields populate with all values defined in the template.

- Templates available to you correspond to the type of notification you are sending.
- Selection of a template is optional and is used typically when sending to multiple recipients. After selecting a template, you can change any notification values without affecting the template.
- See [“Notification templates” on page 91](#) to learn about field values.

4 To assist with the identification of your notification in reports and logging, complete the **Batch Name** and **Batch Description** fields.

If you selected a template, the template name and description automatically populate the Batch Name and Batch Description.

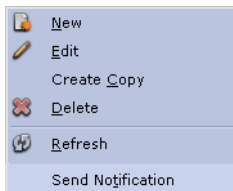
5 Use the **To** field to define the notification recipients. See [“Assigning notification recipients” on page 104](#) to learn more.

6 To choose the installation packages for all Package URL variables in the notification, click **Select Packages**.

For OMA CP notifications, you will find the **Select Packages** button on the Homepage URL page.

The Select Packages for URLs dialog box displays.

Home > Client Deployment > Send Message > Select Packages



- 7 Assign a package for each package URL variable provided on the dialog box, and then click **OK**. Although the package URLs will be added to the message upon sending, you will continue to see the package URL variables.
 - Package URL selection is required for a Message notification.
 - Package URL selection is required for any notification containing a package URL variable. If the message contains package URL variables, you will be unable to send the notification until you have completed all package assignments.
 - Only published packages populate package lists.
- 8 Click **Validate**. The system verifies that all recipient addresses are in the address book. See [“Validating an address” on page 106](#) to learn more.
- 9 To initiate notification delivery, click **Send**. The Sending Client Notifications dialog box displays. See [“About notification delivery” on page 107](#).

Sending notifications based on a template

- 1 In the left pane of the Client Deployment page, select the type of template you want to use. All templates for the type selected display in the right pane.

Home > Client Deployment > Send Notification

- 2 Right-click one of the templates displayed, and then select **Send Notification**.

The Send Notification Message window displays and automatically populates fields with all values defined in the template. See [“Notification templates” on page 91](#) to learn about field values.

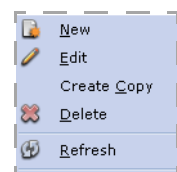
- 3 Use the **To** field to define the notification recipients. See [“Assigning notification recipients” on page 104](#) to learn more.

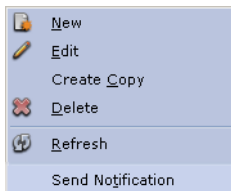
- 4 To choose the installation packages for all Package URL variables in the notification, click **Select Packages**.

For OMA CP notifications, you will find the **Select Packages** button on the Homepage URL page.

The Select Packages for URLs dialog box displays.

Home > Client Deployment > Send Message > Select Packages





- 5 Assign a package for each package URL variable provided on the dialog box, and then click **OK**. Although the package URLs will be added to the message upon sending, you will continue to see the package URL variables.
 - Package URL selection is required for a Message notification.
 - Package URL selection is required for any notification containing a package URL variable. If the message contains package URL variables, you will be unable to send the notification until you have completed all package assignments.
 - Only published packages populate package lists.
- 6 Click **Validate**. The system verifies that all recipient addresses are in the address book. See [“Assigning notification recipients” on page 104](#) to learn more.
- 7 To initiate notification delivery, click **Send**. The Sending Client Notifications dialog box displays. See [“About notification delivery” on page 107](#).

Assigning notification recipients

The assignment of recipients is required to send a notification. Assignment occurs when sending notifications based on addresses, distribution lists, and templates, as well as when sending access point definitions. See [“Sending notifications” on page 101](#) and [“Sending an access point to devices” on page 109](#) to learn more.

To enter recipient addresses:

Enter one or more addresses in the field provided. Delimit multiple addresses with commas.

Home > Client Deployment > Addresses > Send Message

When entering addresses manually, be sure to use recipient validation. You cannot send notifications to addresses that are not in the address book. See [“Validating an address” on page 106](#) to learn more.

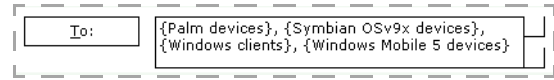


To enter distribution lists:

Enter one or more distribution lists in the field provided. Enclose the distribution list name with braces {}. Delimit multiple lists with commas.

Home > Client Deployment > Distribution Lists > Send Message

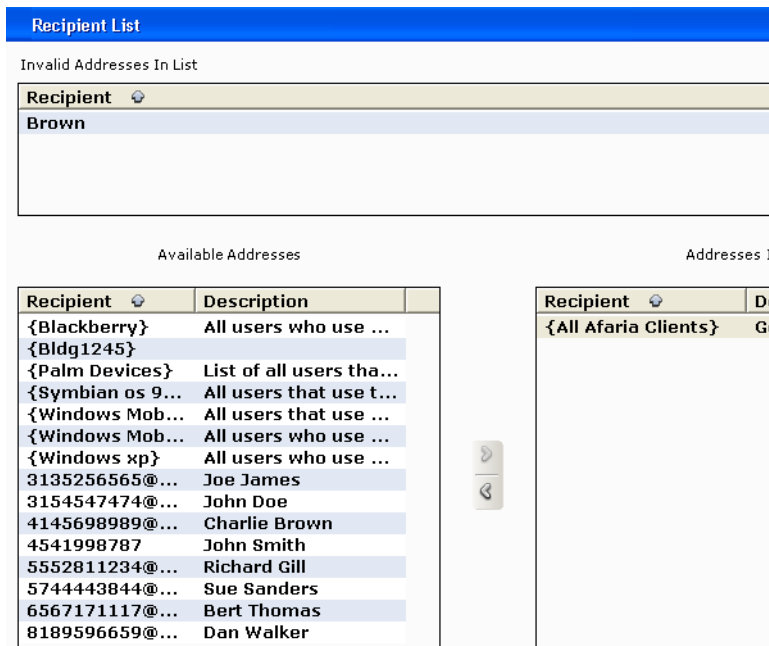
When entering distribution lists manually, be sure to use recipient validation. You cannot send notifications to addresses that are not in the address book. See [“Validating an address” on page 106](#) to learn more.



To select recipients from the address book:

- 1 Click the **To** button. The system validates any addresses already in the **To** field, and then displays the Recipient List dialog box.

Home > Client Deployment > Send Message > To > Recipient List



- 2 Use the arrows to move addresses between the lists.
 - Any invalid recipients you may have entered manually display in the **Invalid Addresses List**. Right-click an entry in this list, and then select **Delete** from the shortcut menu to remove it.
 - To import addresses, click **Import**. See [“Importing addresses” on page 89](#) to learn more.
 - To learn about how the use of a mobile number in the Address affects notification routing, see [“SMS Gateway” on page 144](#).
 - To learn about how the use of a recipient identifier in the Address affects notification routing, see [“SMTP” on page 158](#).
- 3 Click **Save**. The system closes the Recipient List dialog box.

Validating an address

Validation of addresses is not required prior to sending a notification, although the system validates addresses automatically when you attempt to send your message. See [“Sending notifications” on page 101](#) to learn more.

To validate addresses:

Click **Validate** on the Send Notification Message window. The system checks all addresses in the **To** field against the address book entries.

If all addresses validate correctly, the Recipients Validated dialog box displays to inform you of successful validation. Click **OK** to return to the Send Notification Message window.

If any addresses fail validation, the Recipient Validation dialog box displays.

Home > Client Deployment > Send Message > Validate > Recipient Validation

Recipient Validation	
Invalid Addresses	
Recipient	6654455545.
Valid Addresses not in Address Book	
Add	Recipient
<input checked="" type="checkbox"/>	6574355525@cingularme.com
Valid Recipients	
Recipient	6567171117@mycompany.com

To correct an invalid address:

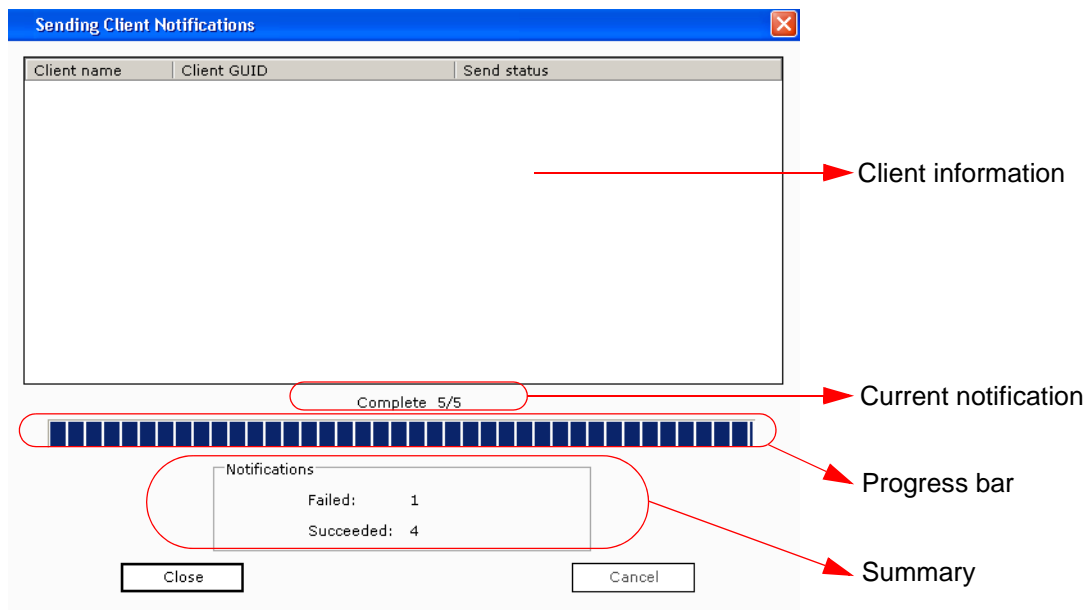
- 1 Double-click on the name in the **Invalid Addresses** list to open the Address Edit Dialog box.
- 2 Make corrections and click **Save**.
 - The corrected address is validated and appears in the **Valid Addresses not in Address Book** list.
 - A check appears in the **Add** column by default indicating that the validated address will be added automatically to the address book.
- 3 Click **Save** to display the corrected addresses in the **To** field of the Send Notification Message window.

Valid Addresses not in Address Book	
Add	Recipient
<input checked="" type="checkbox"/>	3134532342
<input checked="" type="checkbox"/>	6574355525@cingularme.com

About notification delivery

After clicking **Send** on the Send Notification Message dialog box or the Send Access Point dialog box, Afaria progressively summarizes the success or failure status for all notifications.

Home > Client Deployment > Send Message > Sending Client Notifications



The Sending Client Notifications dialog box provides the following information.

- **Client information** – This list does not populate for client deployment.
- **Current notification** – Displays the notification being processed. The information includes the state (e.g., “Notifying” or “Complete”), the recipient address, and its sequence relative to the total group of notifications being sent. For example, in the dialog box shown the system is processing notification 24 in a group of 36 notifications.
- **Progress bar** – Indicates status for processing the complete group of notifications. The progress bar does not imply success or failure for notifications, either individually or collectively, but the progress for processing the notification group.
- **Summary** – Reports the **Send status** totals for all notifications sent. All failures are captured in the Messages log.



Afaria reports only the **Send status** for delivery of notifications to either the SMS Gateway (see [“SMS gateway status” on page 146](#)) or the SMTP server (see [“SMTP” on page 158](#)). The ultimate success or failure of delivery depends on additional components beyond the scope of your Afaria solution.

For example, the ability of the SMSC to receive and relay messages delivered by the SMS Gateway cannot be determined. Nor can the ability of devices to receive messages from wireless carriers be determined, such as when devices are powered off or outside of service areas. Although the send status may indicate success, you cannot assume a device has received a notification.

Self-service portal settings

Use the self-service portal settings if you plan to use notification messages in conjunction with a custom-developed, self-service portal. The settings provide the ability to define access points, device types, and device platforms. The settings you create are available for you to use through the self-service portal.

Access point properties

Access points define a network configuration. Use access points in conjunction with:

- OMA CP templates and notifications, as predefined access points.
- Devices, to package a definition as an OMA CP message and send directly to the device.
- Your self-service portal.

After adding an access point, you can edit, copy, or remove the entry. Each access point has the following properties.

Network service types – GPRS properties

GPRS properties provide access to a General Packet Radio Service (GPRS) network. Use of a GPRS network for the access point precludes the use of a GSM / CSD network.

Home > Client Deployment > Access Points > GPRS

- **Use** – Select to use GRPS as the access type.
- **Defined access points** – Select to apply a predefined GPRS access point definition to the current access point. After applying a predefined access point you can modify the settings.

The remaining data values are defined by your GPRS service provider, which may not require all available fields.

The screenshot shows a configuration form for GPRS. At the top, there is a checked checkbox labeled 'Use' and a button labeled 'Defined access points...'. Below this is a section titled 'GPRS Data' containing several input fields and radio buttons. The fields are: 'Access point name' with the value 'allcellular', 'User name' with the value 'deviceusers', 'Password' with the value '*****', and 'Password (confirm)' with the value '*****'. The 'Authentication type' section has three radio buttons: 'Standard PAP' (which is selected), 'Secure CHAP', and 'Secure MS-CHAP'.

Network service types – GSM / CSD properties

GSM / CSD properties provide access to a Global System for Mobile communications (GSM) / Circuit Switched Data (CSD) network. Use of a GSM / CSD network for the access point precludes the use of a GPRS network.

Home > Client Deployment > Access Points > GSM / CSD

- **Use** – Select to use GSM / CSD as the access type.
- **Defined access points** – Select to apply a predefined GSM / CSD access point definition to the template. After applying a predefined access point you can modify the settings.

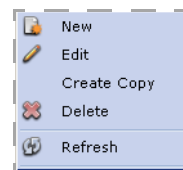
The remaining data values are defined by your GSM / CSD service provider, which may not require all available fields.

Use Defined access points...
ISP for GSM / CSD Data
Phone number 18005551212
Call type Analog ISDN
Call speed 43200
User name JamesJones
Password *****
Password (confirm) *****
Authentication type Standard PAP Secure CHAP Secure MS-CHAP

Sending an access point to devices

Use the send feature to package an access point definition as an OMA CP message and deliver it to devices that support OMA CP. This procedure is a method of provisioning just the access point on a device, without any additional properties. The use of PINs is not supported when sending an access point. If a device requires a user or network PIN, the message will not be accepted by the device.

- 1 From the Client Deployment area, click **Access Points**.
- 2 Right-click the entry in the **Access Points** list, and then click **Send Access Point** from the shortcut menu. The Send Access Point dialog displays.
- 3 Use the **To** field to define the access point recipients. See [“Assigning notification recipients” on page 104](#) to learn more.
- 4 Click **Validate**. The system verifies that all recipient addresses are in the address book. See [“Validating an address” on page 106](#) to learn more.
- 5 To initiate access point delivery, click **Send**. The Sending Client Notifications dialog box displays. See [“About notification delivery” on page 107](#).



Platforms and device types

Device type to platform relationship

The use of device types is optional; the purpose of the device type is to identify a specific platform.

Device types do not function independently of platforms. It is the platform, not the device type, which lets you determine:

- Which installation package the device uses.
- Whether or not a device supports OMA CP.

Supported platform properties

Define supported platforms for use with a custom-defined self-service portal. The list of supported platforms is available through the self-service portal.

After adding a platform, you can edit, copy, or remove the entry. In addition you can build device types based on the platform. See [“Supported device type properties” on page 111](#) to learn more.



Try to provide user-friendly and descriptive names for each platform.

Each platform has the following properties.

Home > Client Deployment > Supported Platforms

- **Name** – A unique name for the platform.
- **Description** – Any additional text you need to further identify the platform.
- **Supports OMA CP** – Select if the platform supports OMA CP notifications.
- **Install Package** – Assign an installation package published to the OTA Deployment Center that will be used for the platform.

The screenshot shows a dialog box titled "Edit Supported Platform". It has a "Name" field containing "WM-Pro", a "Description" field containing "Windows Mobile Professional 6.0", a checked checkbox for "Supports OMA CP", and an "Install Package" dropdown menu showing "Setup_WM6Pro-111.exe - <0000D1C2>". There are "Save" and "Cancel" buttons in the top right corner.

Supported device type properties

Define supported device types for use with a custom-defined self-service portal. The list of supported device types is available through the self-service portal. You must associate each device type with a platform; see [“Supported platform properties” on page 110](#) to learn more.

After adding a device type, you can edit, copy, or remove the entry.



Try to provide user-friendly and descriptive names for each device type.

Each device type has the following properties.

Home > Client Deployment > Supported Device Types

- **Name** – A unique name for the device type.
- **Description** – Any additional text you need to further identify the device type.
- **Platform** – Select a predefined platform family to which the device belongs.

The screenshot shows a dialog box titled "Edit Supported Device Type". It has a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Name:** A text input field containing "WM Professional".
- Description:** A text area containing "Windows Mobile Professional 6.0 Devices".
- Platform:** A dropdown menu currently showing "WM-Pro".
- Buttons:** "Save" and "Cancel" buttons are located to the right of the Name and Description fields.



6

Server configuration

The server configuration area of the Afaria Administrator lets you define parameters for the Afaria Server. Parameters include system-wide application settings, communications options, server schedules, and component configuration.

Properties

In the Properties area of the Afaria Administrator, you can define system-wide parameters for your Afaria Server.

Server Configuration > Properties

Notice the left pane contains several links. Each link opens a different property page.



If you change any values on the property pages, you must stop and restart the Afaria Server in order for the changes to take effect.

The local navigation links are subdivided into functional areas: Communications, Server, and Component configuration.

Communications

In the Communications area, you configure parameters for communication sessions with your Afaria Clients. These parameters include:

- [“Bandwidth throttling” on page 115](#)
- [“Compression” on page 117](#)
- [“Client communication” on page 119](#)
- [“Differencing” on page 128](#)
- [“Server identification” on page 131](#)

Server

In the Server area, you configure the following parameters for Afaria Server information and behavior:

- [“Contact” on page 132](#)
- [“Failed session cleanup” on page 133](#)
- [“License” on page 134](#)
- [“Logging policy” on page 135](#)
- [“Log cleanup” on page 138](#)
- [“OMA DM and Relay Server” on page 139](#)
- [“OTA Deployment Center” on page 142](#)
- [“SMS Gateway” on page 144](#)
- [“Security” on page 152](#)
- [“SMTP” on page 158](#)
- [“User defined fields” on page 159](#)

- [“Outbound notification” on page 161](#)
- [“Relay server” on page 163](#)

SMS Gateway and SMTP configuration properties impact Afaria-initiated messaging. See [“Addresses and routing for Afaria messages” on page 150](#) to learn more about message routing.

Component Configuration

You can configure global settings for the following components:

- [“AV/Firewall” on page 169](#)
- [“Backup Manager” on page 170](#)
- [“Document Manager” on page 171](#)
- [“Exchange ActiveSync policy” on page 172](#)
- [“Manager for SMS” on page 179](#)
- [“Patch Manager” on page 185](#)

Bandwidth throttling

When you enable bandwidth throttling, you can increase or decrease the communications rate (measured in bits per second) throughout the course of a Client session, allowing Client users to run other network applications more effectively when they communicate with the Afaria Server.

Server Configuration > Properties > Bandwidth Throttling

Use bandwidth throttling to increase or decrease the communications rate throughout the course of a Client session.

Enable bandwidth throttling

Enable calibration

Enable event logging

Configurations

Current default:

[New...](#) [Delete...](#) [Set default...](#)

Client throughput

Specify these values to set a "ceiling" and a "floor" throughput rate which the Server will maintain during a client communications session.

Minimum: Kbps


Maximum: Kbps

Throttle down

Threshold: Indicates percentage of activity below which throughput must fall for throttling to occur.

Wait time: Indicates the amount of time (in seconds) the Server will wait before throttling down communication activity.

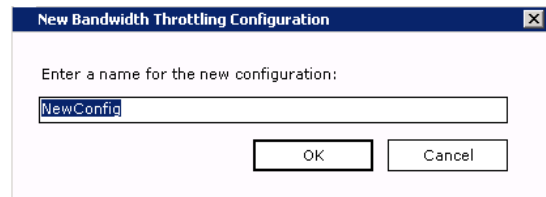
Percent: Indicates the percentage of current throughput to which the Server will throttle down communication.

 You must restart the Service to use any new values.

On the Bandwidth throttling page, you'll see the following fields and options:

- **Enable bandwidth throttling.** Enables bandwidth throttling on the server and enables all the fields on the Bandwidth throttling page. Bandwidth throttling must be enabled on all servers in a server farm environment if you intend to use bandwidth throttling features in any of the channels you replicate.
- **Enable calibration.** Allows you to modify configuration parameters without having to stop and restart the server service in order for changes to take effect. Enabling calibration will also cause the server to log bandwidth throttling information to the Messages log view at the end of a session.
- **Enable event logging.** Enables bandwidth throttling events to be raised in the alerts subsystem.

- **Configurations area.** The Current default field displays the default configuration. The server automatically defaults to 100 Mbps bandwidth throttling capabilities. You can select a different configuration from the drop-down list, or you can click the **New** link to create a new configuration. The New Bandwidth Throttling Configuration dialog box appears and allows you to name a new configuration. You can delete any configuration you create by selecting it from the drop-down list and clicking **Delete**. You can make any configuration in the list the default configuration by selecting it from the drop down and clicking **Set Default**.



The image shows a dialog box titled "New Bandwidth Throttling Configuration". It has a blue title bar with a close button (X) in the top right corner. The main area contains the text "Enter a name for the new configuration:" followed by a text input field containing "NewConfig". Below the input field are two buttons: "OK" and "Cancel".



Using a bandwidth configuration set at 14.6 kps, in conjunction with 10-minute or greater channel delivery segmentation criteria, may result in dropped connections.

- **Client throughput area.** In this area, you can specify the Maximum and Minimum throughput rate (Kbps) the server should maintain during a Client session.
- **Throttle down area.** In this area, you can set three values:
 - *Threshold.* The percentage of activity below which throughput must fall for throttling to occur.
 - *Wait time.* The number of seconds the server should wait before throttling down communication activity with Clients.
 - *Percent.* The percentage of current throughput to which the server should throttle down communication with Clients.




If you enter a value of 0 (zero) in the Percent field, bandwidth throttling will never occur; the server will not take action and will function as though this feature were not present.

Compression


From the Compression page, you can view the cache of compressed files that are frequently sent to Clients. This reduces connection time and improves system performance. By default, the Afaria Server uses ten percent of the disk space for the compressed file cache, but you can specify a different percentage using the slider bar.

Server Configuration > Properties > Compression


 The compression cache stores files that are frequently sent to Clients. Cached files are compressed to reduce connection time and improve system performance. [View cache ...](#)

Date of last refresh: 12/4/2008 12:00 AM [Refresh now](#)

Disk space

Amount of disk space to use:  10% of drive [Empty cache](#)

Remove files from the cache if the source file is not found during a refresh

 You must restart the service to use a new disk space value. Note: Files less than 16384 bytes in size are not cached.

Select the “**Remove files**” check box if you want to delete a file from the list of files that Afaria attempts to cache when Afaria cannot find the file during a refresh action. It is recommended that you store your cached files locally when using this option in order to prevent occurrences of network access outages from unintentionally causing Afaria to delete files that you would prefer to keep.

If you want to view a list of the files in the compression cache or add files to the compression cache, you can click the **View Cache** link. This opens the Compressed file cache window.

Compressed file cache							
Source file	Cached file	Type	Source size	Cached size	Ratio	Last accessed	Last checked
C:\Progra...		No...	12,568,554	0	***	12/4/2008 14...	12/2/2008 15...
C:\Progra...	C:\Progra...	No...	216,064	113,154	47....	11/24/2008 1...	11/24/2008 1...

You can sort the information in the Compressed file cache window by clicking the column headings. The total number of files in the cache appears at the bottom of the window, along with the amount of disk space used.







You can also view the amount of disk space used by the Compression cache on the server status page in the Home area of the Administrator.

The Compressed file cache window lists the following information about cached files:

- **Source file.** The location of the source file on the network.

- **Cached file.** The location of the cached file on the network.
- **Type.** Displays as Normal.
- **Source size.** The size (in bytes) of the original file.
- **Cached size.** The size (in bytes) of the cached file on the server.
- **Ratio.** The percentage difference between the source file and the cached file.
- **Last accessed.** The date and time the file was added to or updated in the compression cache.
- **Last checked.** The date and time the file was last checked by the system.

From the Compressed file cache window, you can complete the following actions by clicking the corresponding toolbar button listed in the table below:

<i>Click</i>	<i>To do this:</i>
	Add files to the compression cache.
	Remove a file from the compression cache.
	Refresh the data in the compression cache.
	Refresh the file list in the Compressed file cache window.

See “[Server schedules](#)” on [page 186](#) for information about the compression refresh schedule.

Client communication

Use the Client Communication page to configure communication between the Afaria Server and your Afaria Clients¹. You can configure communication for encrypted sessions, server authentication, and client authentication. Client communication settings define session protocol and ports, manage the server's SSL certificate, and define the server address seed value for clients.

Server Configuration > Properties > Client Communication

Protocols and ports

Configure protocols and ports to use for client communication. XNET is always used. Ensure your firewall allows bidirectional traffic for each port used.

<input checked="" type="checkbox"/> XNET (TCP/IP)	Port	<input type="text" value="3007"/>	Reset to default
<input type="checkbox"/> XNETS (TCP/IP over SSL)	Port	<input type="text" value="3008"/>	Reset to default
<input checked="" type="checkbox"/> HTTP	Port	<input type="text" value="80"/>	Reset to default
<input checked="" type="checkbox"/> HTTPS	Port	<input type="text" value="443"/>	Reset to default

Certificate settings

To use the XNETS and HTTPS protocols, you must associate the certificate obtained from a Certificate Authority (CA) with the corresponding private key and password.

[View...](#) [Settings...](#)

[Associate key and password...](#) [Generate request...](#)

Address for Client communication

Define the default server address for Clients to use when contacting the server. This value is used to seed client installations, XEC generation, and outbound notifications. Resetting the default address will select the port number from above.

Syntax: [protocol://]Address[:port]
Example: 10.24.23.13
Example: xnets://server1.example.com:3008

[Reset to default...](#)

Setting Protocols and Ports

Define the communication protocol and server ports for bidirectional session traffic that occurs between the server and clients. Ensure that your firewall allows the traffic you enable.

Enable SSL when your enterprise requires encryption or authentication for server/client sessions. However, be advised that SSL adds payload to sessions.

- 1 Begin on the Server Configuration Client Communications page.

1. OMA DM Clients, in contrast to Afaria Clients, are seeded with OMA DM server address information. See “OMA DM and Relay Server” on page 139.

- 2 Select the protocol and define the port, according to your organization's requirements:
 - XNET – TCP/IP protocol that is optimized for Afaria communications.
 - XNETS – TCP/IP over SSL.
 - HTTP – HTTP protocol. If you have Afaria Administrator installed on the same server with other applications, such as other IIS applications, ensure the port you use does not conflict with the other applications.



- The Afaria Server service does not start if the HTTP port is configured for 1025, 1026, or 1027.
 - If HTTP port contention occurs with another application, the first application to start may operate, while the second application may fail.
 - Before beginning optional relay server operations, validate that clients can connect directly to the server using HTTP.
- HTTPS – HTTP over SSL for secure communications.

Click **Reset to default** at any time to return to the default port number.

Defining the Server Address for Client Communication

Define the default server address for clients to use when contacting the server. This value is used in several contexts.

- Client package seed data – The Afaria Create Client Install program uses this value to seed new clients with a server address. You can override the seed value, if you need a different value when you make a client package.
- HTML-based channels – Clients that run channels that you create based on the channel administration's HTML code generator, XEC channels, use the address to initiate connections to the server.
- Outbound notifications – The server initiates outbound notifications that include the server address. Responding clients use the address from the notification to initiate a connection back to the server.

The address may be for the Afaria Server, the optional relay server, or some other intermediary server your clients connect to for initiating sessions.

- 1 Begin on the Server Configuration Client Communications page.
- 2 Click **Reset to default** to populate the address with the IP address and your protocol selection, or type the fully qualified host name or IP address of the server.

The address uses syntax:

`[protocol://]address[:port]`

Afaria Server and Client Authentication

The product supports both server authentication and client authentication.

- Server authentication – The client requests a certificate from the server during the communication handshake to verify that the server is trusted. Server authentication prevents a rogue server from intercepting communications between the client and the intended server.
- Client authentication – The server requests a certificate from the client during the communication handshake to verify that the client is trusted. Client authentication prevents rogue devices from running sessions with the server.

The certificate verification includes verifying that the certificate is from a trusted certificate authority (CA), the server or client's identity for configured values, and the certificate's expiration date.

Server SSL Certificate Requirements for Server Authentication

A signed server SSL certificate represents a trusted server identity for clients. For installations that implement server authentication, SSL sessions run only when the client evaluates the server's certificate as valid, as evaluated against 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)
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).
 - Personal Information Exchange (.PFX)
- The certificate key is an RSA key.

Client SSL Certificate Requirements for Client Authentication

A signed client SSL certificate represents a trusted client identity for the server. For installations that implement client authentication, the product allows SSL sessions to run only when the server evaluates the client's certificate as 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 following certificate fields match the server's configuration for the corresponding fields:
 - Organization – corresponds to the "Organization" data element on the Client Communication page's Certificate Settings dialog.
 - (Optional) Organizational Unit – corresponds to the "Organizational Unit" data element on the Client Communication page's Certificate Settings dialog.
- The certificate is valid for encryption and authentication.
- The certificate is compliant with x.509 certificate standards. Supported format is type Personal Information Exchange (.PFX).
- The certificate key is an RSA key.

Implementing Server Authentication

Supported client types – BlackBerry, Symbian, Windows, Windows Mobile Professional, Windows Mobile Standard

Configure your server and clients for server authentication when you want the clients to request a certificate from the server to verify that the server is trusted.

- 1 Install your signed server SSL certificate.

Generate a certificate request if you do not already have one.

- 2 If your client devices do not already have a certificate for the trusted CA that is at the top of the server certificate's signing chain, deploy the CA certificate to clients. Consider the following items:

- The client requires a Base64-encoded x.509 (.CER) certificate.

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).

- Most clients have commercial CA certificates already in place in their certificate store. Consult your device product documentation to learn about which CA certificates are available on the device.
- (Symbian, BlackBerry) The CA certificate must reside in the certificate store.
- (Windows, Windows Mobile) The CA certificate must reside in either the certificate store or Afaria Client's In folder (path <ClientInstallDirectory>\Data\Certs\In).

- 3 (Optional) Define the server configuration for SSL session encryption.

- 4 Set the SSL protocol and port according to your organization's requirements.

- 5 Restart the server.

- 6 Connect clients.

Denied connections are logged in the Messages log.

Implementing Client Authentication

Supported client types – BlackBerry¹, Symbian¹, Windows, Windows Mobile Professional, Windows Mobile Standard

Configure your clients and server for client authentication when you want the server to request client certificates to verify that each client is trusted. Implement client authentication only after you implement server authentication.

- 1 Deploy a signed client SSL certificate to each client that you want the server to authenticate.
 - (Symbian, BlackBerry) Deploy the certificate to the certificate store.
 - (Windows, Windows Mobile) Deploy the certificate to a user-defined location.

When you request the certificate, make note of the deployment location, file name, and certificate's password; these values are required for configuring the clients.

- 2 Configure your Afaria clients with values for the certificate path and file name and the certificate's password.

You can manually configure existing clients. You can configure new clients with the values as seed data by using the Afaria Create Client Installation program's Client Certificate page.

- 3 Copy the certificate for the trusted CA that is at the top of the client certificate's signing chain to server path: <ServerInstallDirectory>\Data\Certs\In.
- 4 Define the server configuration for client authentication.
- 5 Restart the server.
- 6 Connect clients.

Denied connections are logged in the Messages log.

Generating a Request for a Server SSL Certificate

Generate a request for a server certificate when you do not already have a valid certificate installed on the server and plan to implement either server authentication or session encryption without server authentication. This feature also generates an encryption key for the server.

The certificate request feature is just one of many ways for you to generate a certificate request. You may prefer to use other resources, such as a certificate authority's (CA) request processes or open-source SSL tools to facilitate creating a server key and request.

- 1 On the Server Configuration Client Communications page, click **Generate Request** to launch the request wizard.

1. The BlackBerry and Symbian platforms require users to interact with their device to facilitate client authentication. Test devices in your environment to understand the user requirements.

- 2 On the Personal Data page, complete the data for your organization, then click **Next**.
For server authentication, you must define the “Common Name” with the value that you plan for your clients to use to initiate connections with the server. This value is typically a fully qualified domain name.
- 3 On the Key Data page, select your encryption-key size and enter a password, then click **Next**.
Retain this password for later use to install the certificate.
- 4 On the File Data page, define the paths and file names for storing the request file and key file, then click **Next**.
File extensions .CRQ and .KEY are suggested for the request and key files, respectively.
- 5 Review the summary page.
- 6 Click **Finish**.
The wizard produces a request file and a key file. Send the request file to your commercial CA or your self-signing authority.

Installing the Server’s SSL Certificate

Install a signed server SSL certificate when implementing server authentication or encryption without server authentication. The installation process creates the server identity file, which the server uses during operations. The server identify file associates a certificate, an encryption key, and a password into a single file. A server uses only one server identity file.

- 1 On the Server Configuration Client Communications page, click **Associate Key and Password** to open the Create Server identity dialog box.
- 2 In the Certificate File area, enter the path and file name for the server certificate.
- 3 (CER type certificates) In the Private Key File area, enter the path and file name for the server’s private encryption key.
The Client Communications page’s Generate Request feature can create the key, as can other generally available resources.
- 4 (CER type certificates) In the Server Identity File area, enter a file name for the server to use to create an identity file.
- 5 In the Server Identity File area, enter and confirm an associated password.
- 6 Click **OK**.

The server associates the certificate and key and saves it into an encrypted server identity file. The server uses the password to access the certificate to present it at authentication time. Do not change the server identity file’s location or name.

Viewing the Server's SSL Certificate

View a certificate to review details about a server's SSL certificate. The certificate details are contained within the server identity file, created when you installed the server's certificate. The server uses only one identity file.

- 1 On the Server Configuration Client Communications page, click **View**.

The certificate list includes the following data elements:

- Issued to – The name of the organization to which the certificate was issued.
- Issued by – The name of the certificate authority that issued the certificate.
- Expiration – Certificate's expiration date.
- Key type – The key type associated with the certificate.

- 2 Select the certificate of interest.

The certificate details list includes the certificate's fields and values.

Selecting SSL options for Session Encryption

Select SSL options to disable specific encryption ciphers from the product's use. The product uses SSL and TLS cryptographic protocols, and supports using cipher suites that comply with FIPS 140-2 standards and a variety of other industry-standard suites. The null cipher suite is not supported.

At connection time, the session uses the strongest cipher suite that is supported by both the server and the client.

- 1 On the Server Configuration Client Communications page, click **Settings**.
- 2 In the SSL/TLS Options area, define the options according to your organization's requirements:
 - FIPS 140-2 only – Disable all ciphers that do not comply with FIPS 140-2 standards.
 - Disable MD5 ciphers – Disable MD5 ciphers. Disable MD5 ciphers unless you have legacy devices that do not offer stronger options.
- 3 Click **OK**.

Configuring the Server for Client Authentication

Configure the server to define whether client authentication is required for sessions, and which certificate field values to use for authenticating clients.

- 1 On the Server Configuration Client Communications page, click **Settings**.

- 2 In the Client Certificate area, define the authentication settings according to your organization's requirements:
 - Require certificate – Require client authentication for all sessions. If required, the server runs session only if authentication is successful. If not required, the server runs session regardless of client's certificate state.
 - Organization – Enter the value used for "Organization" on the signed client certificates.
 - (Optional) Organizational Unit – Enter the value used for "Organizational Unit" on the signed client certificates.
- 3 Click **OK**.

Uninstalling the Server's SSL Certificate

Uninstall a server's certificate to remove it from the server and discontinue its use for server authentication. SSL connections that occur while the server is without a certificate are denied.

- 1 On the Server Configuration Client Communications page, click **View**.
- 2 Select the certificate of interest.
- 3 Click **Remove**.

Changing the Password for your SSL Certificate

Change the password associated with your signed server certificate as your requirements dictate. Continuing with server authentication after changing the password for a server certificate requires no further action.

- 1 Begin on the Server Configuration Client Communications page.
- 2 Click **View**.
- 3 Select the certificate of interest.
- 4 Click **Change Password**.
- 5 Enter the current password.
- 6 Enter and confirm the new password.
- 7 Click **OK**.

Configuring Session Encryption without Authentication

Supported client types – Java, Palm

Configure your server for encryption without authentication when you want SSL-encrypted sessions for clients that do not support server or client authentication.

Encrypting traffic between the server and its clients requires a signed server certificate and SSL protocol. You can benefit from encrypted sessions even when you are not using server or client authentication.

- 1 Set the SSL protocol and port according to your organization's requirements.
- 2 Associate your server's signed certificate and key before beginning encrypted sessions.

If you run encrypted sessions without authentication, you are strongly advised to strengthen your security implementation by also enabling user authentication at the server and for all channels.

See also ["Security" on page 152](#) and ["Channels – Security Tab" on page 296](#).

Differencing

You use the Differencing cache to maintain different versions of files that you frequently send to Afaria Clients; the Afaria Server will send only the updated bytes of each file in the differencing cache. By default, the server uses ten percent of the disk space for the file differencing cache, but you can specify a different percentage.



Each cached file at the server maintains a maximum of 32 differences.

Server Configuration > Properties > Differencing

A screenshot of a configuration dialog box for the Differencing cache. The dialog has a dashed border and contains the following elements: a document icon with text explaining the cache's purpose and a 'View cache...' link; a 'Date of last refresh' field showing '12/4/2008 12:01 AM' and a 'Refresh now' link; a 'Disk space' section with a slider set to '10% of drive' and an 'Empty cache' link; a checkbox labeled 'Remove files from the cache if the source file is not found during a refresh' which is currently unchecked; a warning icon and text stating 'You must restart the service to use a new disk space value. Note: Files less than 16384 bytes in size are not cached.'; and 'Save' and 'Cancel' buttons at the bottom.

Select the “**Remove files**” check box if you want to delete a file from the list of files that Afaria attempts to cache when Afaria cannot find the file during a refresh action. It is recommended that you store your cached files locally when using this option in order to prevent occurrences of network access outages from unintentionally causing Afaria to delete files that you would prefer to keep.

Disk space setting and the total cache size

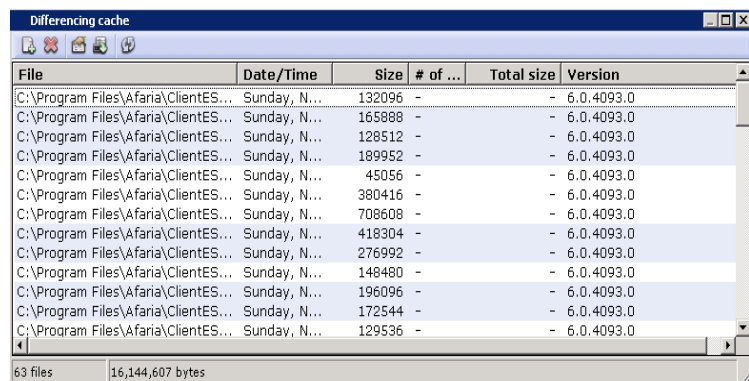
Total cache size – Afaria determines whether the cache content size exceeds the cache size setting before it adds a new differencing file. If the total cache size is within the defined disk space allocation before it adds a new differencing file, Afaria will add a new file to the cache without removing any existing files from the cache. Therefore, it is possible for the cache size to cross the allocated threshold with the addition and exceed the disk space you allocated. If the total cache size exceeds the defined disk space allocation before it adds a new differencing file, Afaria will add a new file to the cache and remove one or more of the least recently used files to bring the total cache size to within the defined disk space that you allocated.

Reducing the disk space setting – Afaria can reduce the current disk space setting only as much as the current total cache size. For example: If you have the disk space set to 10% and decide to reduce it to 5% but have 7% worth of cached data, Afaria sets the disk space at 7% after you stop and restart the service, not the 5% that you set. If you first empty the cache or manually reduce the total cache size by deleting items from the cache before you reduce the disk space setting, then the reduced setting can go into effect once you stop and restart the service.

Viewing the cache

If you want to view a list of the files in the differencing cache, or add files to the differencing cache, you can click the **View cache** link. This opens the Differencing cache window.

You can sort the information in the Differencing cache window by clicking the column headings. The total number of files in the cache appears at the bottom of the window, along with the amount of disk space used.



File	Date/Time	Size	# of ...	Total size	Version
C:\Program Files\Afaria\ClientES...	Sunday, N...	132096	-	-	6.0.4093.0
C:\Program Files\Afaria\ClientES...	Sunday, N...	165888	-	-	6.0.4093.0
C:\Program Files\Afaria\ClientES...	Sunday, N...	128512	-	-	6.0.4093.0
C:\Program Files\Afaria\ClientES...	Sunday, N...	189952	-	-	6.0.4093.0
C:\Program Files\Afaria\ClientES...	Sunday, N...	45056	-	-	6.0.4093.0
C:\Program Files\Afaria\ClientES...	Sunday, N...	380416	-	-	6.0.4093.0
C:\Program Files\Afaria\ClientES...	Sunday, N...	708608	-	-	6.0.4093.0
C:\Program Files\Afaria\ClientES...	Sunday, N...	418304	-	-	6.0.4093.0
C:\Program Files\Afaria\ClientES...	Sunday, N...	276992	-	-	6.0.4093.0
C:\Program Files\Afaria\ClientES...	Sunday, N...	148480	-	-	6.0.4093.0
C:\Program Files\Afaria\ClientES...	Sunday, N...	196096	-	-	6.0.4093.0
C:\Program Files\Afaria\ClientES...	Sunday, N...	172544	-	-	6.0.4093.0
C:\Program Files\Afaria\ClientES...	Sunday, N...	129536	-	-	6.0.4093.0

63 files 16,144,607 bytes



You can also view the amount of disk space used by the Differencing cache on the Server status page in the Home area of the Afaria Administrator. For more information, see [“Server status” on page 67](#).

The Differencing cache window lists the following information about cached files:

- **File.** The file name and its path on the server.
- **Date/Time.** The date and time the file was added to the differencing cache.
- **Size.** The size in bytes of the original file in the cache.
- **# of versions.** The number of versions of this file that are in the cache.
- **Total size.** Size of the updates.
- **Version.** The version number of the file.

From the Difference cache window, you can complete the following actions by clicking the corresponding toolbar button listed in the table below:

Click	To do this:
-------	-------------



Click this button to **add files**.



Click this button to **remove a file**.

<i>Click</i>	<i>To do this:</i>
--------------	--------------------



Click this button to **view details** for the selected file.



Click this button to **refresh the data** in the differencing cache.



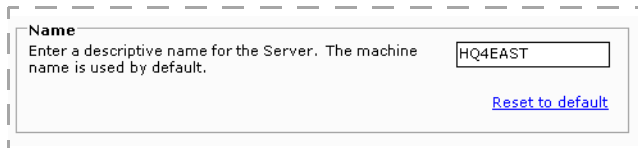
Click this button to **refresh the file list** in the Difference cache window.

See [“Server schedules” on page 186](#) for information about the differencing refresh schedule.

Server identification

You use the Server identification page to set or edit the Afaria Server name. The name is visible to Afaria Windows Client Channel Viewer users.

Server configurations > Properties > Server identification



The screenshot shows a form titled "Name" with the instruction "Enter a descriptive name for the Server. The machine name is used by default." To the right of the text is a text input field containing "HQ4EAST". Below the input field is a blue link labeled "Reset to default". The entire form is enclosed in a dashed border.

Name. A descriptive name for the Afaria Server. The computer name appears by default. You can click **Reset to default** at any time to display the computer name.



The server name cannot include the backslash (\) character.

Contact

The Contact property page lets you provide Afaria Windows Client Channel Viewer users with information regarding the person to contact if they have questions with their Clients or encounter problems during a communication session with the Afaria Server.

Server Configuration > Properties > Contact

Contact information


Enter this information to specify a contact for users that have questions or need assistance. They will see this information in the Channel Viewer in the Server Properties dialog under the Contact tab.

Contact

Phone number

E-Mail

Notes

 You must restart the service to use any new values.

Failed session cleanup

You can use the Failed session cleanup page to control how the system handles failed communication sessions between Afaria Clients and the Afaria Server.

Server Configuration > Properties > Failed Session Cleanup

Failed sessions automatic cleanup

Specify how long the system should keep track of failed sessions. The system keeps track of failed sessions in order to perform session restarts. If you are low on disk space, you might want to decrease this number.

Cleanup every Hour(s) Day(s)


[Reset to default](#)

Failed sessions manual cleanup

If a channel continues to fail despite several attempts on your part to correct it, click View failed sessions and delete that channel entry from the list. This forces the channel to restart from the beginning.

[View failed sessions...](#)

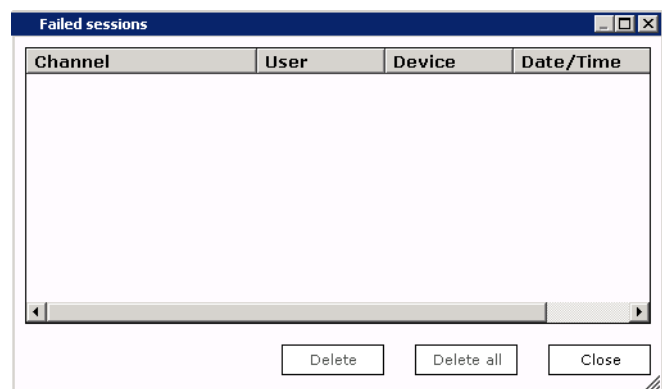
[Clear all failed sessions](#)

 You must restart the service to use any new values.

The **Failed sessions automatic cleanup** option allows sessions to recover from the point at which they were interrupted, if they reconnect within the time you specify. Once that specified time elapses, the server clears all records of failed sessions and any users reconnecting after that occurs must restart their communications sessions from the beginning.

The **Failed sessions manual cleanup** option lets you force a channel to restart a communications session from the beginning rather than from the point at which the session was interrupted. This is particularly useful when a channel continues to fail despite several attempts to correct it.

When sessions continue to fail, you can click **View Failed Sessions** to open the Failed Sessions dialog box, which displays details about the Channel, User, Client, and Time/Date associated with the failed session. You can also delete failed sessions from this dialog box by selecting the channel and clicking **Delete**.



License

The Licensing page contains information about your Afaria system, including a list of licensed components and Afaria Client types, the number of licensed sessions, expiration dates (if any), and a brief description of the license type.



The information on this page is for display only. You cannot modify any values on this page.

Server Configuration > Properties > License

Item	Value
System Serial Number	1
Maximum concurrent sessions	Unlimited
Server was installed on	10/31/2009
Win32 Client	
Win32 Session Manager	Licensed
Win32 Software Manager	Licensed
Win32 Inventory Manager	Licensed
Win32 Document Manager	Licensed
Win32 Manager for MS SMS	Licensed
Win32 Backup Manager	Licensed
Win32 Software Packager	Licensed
Win32 License Manager	Licensed
Win32 Data Security Manager	Licensed
Win32 Patch Manager	Licensed
Palm Client	

License key: 1J-SQCQ-9JPV-UZUS-WGZZ-8X9M-37C9-EM7N-LWDK-UMDL

Logging policy

From the Logging policy page, you can determine the Afaria global logging policy settings for the logs in Data Views. All logs are enabled by default.



Items that are backed up can be managed in Data views, Backup. For detailed information on each of the logging views, see [“Working with Logged Actions” on page 439](#).

Server Configuration > Properties > Logging Policy

Global logging policy settings

Disable all logging

Message logging services

- User
- Information
- Fatal
- Debug
- Error

Replication logging services

- User
- Information
- Fatal
- Debug
- Error

Sessions

- Failed
- Completed
- Successful

Session event details

- Failed
- Successful
- Comments
- Disabled
- Skipped

Client action logging services

- Error
- Successful

Enable alert logging

You must restart the service to use any new values.

Save Cancel

The Logging policy page contains the following fields and options:

- **Disable all logging.** When you select this option, you disable all server logging.
- **Message logging services.** Records information, warning, and error messages specific to the server. You can select this category to log information about when channels were created, modified, published, unpublished, and deleted, when the server service was started and stopped, and when a worklist or sendlist was modified.
- **Replication logging services.** Records replication-specific information, warning and error messages. You can select this category to log information about channels replicated to or from your server, when server partners were added, or when a connection occurred.
- **Sessions.** Records information about past sessions, such as the channel involved, the end time and duration, the user and computer information, and the session event status.
- **Session Event Details.** Records log details at the object level pertaining to File Transfers or Sessions, which you can view via the Detailed History for Session window. which provides a detailed list of channel work objects and allows you to quickly identify the objects executed and any problems that may have started. This is most applicable to Session Manager channels, which may contain multiple Worklist and Sendlist objects. Software Manager and

Document Manager channels generally only consist of one work object that is automatically generated by the server. See [“Best practice: session event details” on page 137](#).

- **Client action logging services.** Records information about actions occurring on the Client. You can select this category to log information about successes or failures, failures only, or nothing at all regarding actions performed on the Client.
- **Enable alert logging.** When you select this option, you enable the server to log both raised events and closed alerts on your server. For raised events, the logs display information such as the name of the event, the computer on which the event occurred, the time the event occurred, and any relevant details. For closed alerts, the logs display information such as the name of the alert, the contact (if any) associated with the alert, the time the alert was acknowledged, or the time the alert was closed.

Log message types

For Messages Logging Services and Replication Logging Services, you can select to make the following types of log entries for relating to server or replication activities:

- **User.** Messages describing user activity.
- **Information.** Messages containing information about normal operations.
- **Fatal.** Messages indicating a critical failure of a server application. You should investigate the source of these errors.
- **Debug.** Messages containing debug or diagnostic information for support or troubleshooting.
- **Error.** Messages indicating usage or formatting errors.

For Session logging, you can select to create a log message for the following types of sessions:

- **Failed.** Sessions that either did not execute successfully or did not complete as expected.
- **Completed.** Sessions that did not execute but may have been skipped by a conditional event.
- **Successful.** Sessions that complete successfully.

For Session Event Detail logging, you can select to create a log message for the following types of session events:

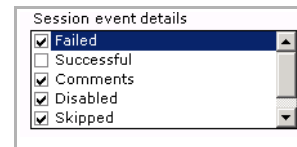
- **Failed.** Events that either did not execute successfully or did not complete as expected.
- **Successful.** Events that complete successfully.
- **Comments.** Comment events.
- **Disabled.** Events with the status value set to “Disable”.
- **Skipped.** Events that are skipped due to conditional logic or due to its irrelevance to the Client type that the event is running on.
- **System.** Events that run as part of the Afaria operations, rather than as part of a channel that you created.

For Client action logging, you can select any of the following message types:

- **Error.** Displays logs for actions occurring in response to an Afaria monitor trigger that ended in with an error status.
- **Successful.** Displays logs for actions occurring in response to an Afaria monitor trigger that ended in with a successful status.

Best practice: session event details

It is considered a best practice to omit successful transactions from logging when you choose to log session event details. Logging successful session event details is a resource-intensive process that can contribute to reducing server response times and can grow your database at an undesirable rate.



Log cleanup

Use the Log cleanup page to specify the cleanup time for the individual logs that display in Data views, Logs. To enable cleanup for a log, select the **Enabled** check box and use the spin box to specify how old a record should be before it is deleted from the log.

Server Configuration > Properties > Log Cleanup

Log	Enabled	Number of days
Message	<input checked="" type="checkbox"/>	30
Session	<input checked="" type="checkbox"/>	30

Log cleanup is available for each of the log types that you can view in Data views. See [“Working with Logged Actions” on page 439](#) for more information about logs. Choose **Reset defaults** to reset the page to the default values.

See [“Server schedules” on page 186](#) for information about the log clean up schedule.

Best practice: cleanup frequency

It is considered a best practice to establish your log cleanup settings to perform cleanup often enough that performing the log cleanup has negligible impact on Afaria performance. This optimum setting varies from organization to organization and must balance with your need for log history.

OMA DM and Relay Server

Use the Afaria OMA DM Server page to define the OMA DM server address properties that OMA DM Clients need to communicate with the OMA DM server. Clients run sessions directly with the OMA DM server. The OMA DM server runs sessions with the Afaria Server as a proxy for the Client.

Configure OMA DM Server

The following property page shows an example of how to configure the OMA DM Server to communicate with the Relay Server.

Server Configuration > Properties > OMA DM Server

Server address

External address

Server Id

Ports


HTTP HTTPS

Relay Server

Farm ID

Client URL prefix

Client uses secure connection to RS

 You must restart the service to use any new address values.

Afaria Clients, in contrast to OMA DM Clients, are seeded with Afaria Server address information. See [“Client communication” on page 119](#).

Server address

Use the Server address group values to define the settings that OMA DM Clients need to communicate with the OMA DM server and which the OMA DM Server uses to communicate with the Relay Server. Use Afaria OMA DM policy features to define new Clients and provision them with these values. See [“Policy Category – OMA DM” on page 259](#).

- **External IP Address.** The External address (which can be an IP address or a domain name) is the address of the Relay Server.
- **Server ID.** The case-sensitive, user-defined ID for your OMA DM server that you used when you installed the OMA DM server and that the Relay Server uses to recognize the OMA DM Server.

- **Ports:**



To specify an OMA DM Relay Server port number, other than the default of "80", you must enter in the Relay Server Client URL prefix, the port number preceded by a colon.

- **HTTP/HTTPS.** The host server's ports for receiving OMA DM HTTP and HTTPS communications. The ports cannot conflict with the Afaria Server HTTP and HTTPS ports, as defined on the Afaria Administrator's configuration page for Client communications.
- **Relay Server:**
 - **Farm ID.** Must match the farm ID configured in the **rs.config** file on the Relay Server.
 - **Client uses secure connection to RS.** Check the box if the client is using a secure connection.
 - **Client URL prefix.** When the device connects using the OMA DM profile, it connects to the Relay Server, which provides the connection data to the server defined by the Server Farm and the Server ID that is defined in the host Address. The Client URL prefix depends on how the Relay Server was installed.

When the device is provisioned using the sample data, the Host Address will be:

```
https://192.168.1.155/ias_relay_server/client/rs_client.dll
```

Starting the Relay Server Outbound Enabler

To start the Relay Server Outbound Enabler connect it to the OMA DM server. This is done by using an application provided with the Afaria Install. The application is the Relay Server Outbound Enabler (**rsoe.exe**) and it can be found in the directory:

```
<Afaria_Base_Install>\bin\RSOutboundEnabler
```

Using the data in the previous example, a sample of the command line to launch the Relay Server Outbound Enabler would be:

```
rsoe.exe -f AfariaFarm -id AfariaOmaDmServ -cr "host=192.168.1.155;port=80"  
-cs "host=10.24.21.220;port=31021" -t abc
```

where:

- f denotes the FarmID
- id denotes the Server ID (which is the OMA DM Server ID)
- cr denotes the address of the Relay Server
- cs denotes the address of the back end server, which is the OMA DM server
- t denotes the security token defined on the Relay Server for this Server ID

Relay Server Outbound Enabler issues:

- The External Address defined in the properties of the OMA DM Server and the address of the Relay Server using the -cr tag, when starting the Enabler, do not have to match. The

Relay Server may present one address to the internal connections (such as the Enabler and OMA DM server) and external connections (such as the device).

- The Enabler must be started after the Relay Server is started because the Enabler verifies the Relay Server address and port when starting.
- A security token is not required. If it is included when the back end server is defined in the **rs.config** file, it must also be included when the Enabler is started.

OTA Deployment Center

OTA is the acronym for “Over The Air.” The Afaria OTA Deployment Center is a Web server that provides software deployment services for your Afaria solution. Using deployment services with your solution is optional. An administrator uses the Afaria OTA Publisher application to push Afaria Client software to the deployment center and then sends notifications to device holders to connect to the deployment center to download the Client installation packages to the device. Device holders download the Client installation packages directly onto their device for installation.

Use the Afaria OTA Deployment Center page to configure the settings that device holders will use to connect to the Client-facing interface and the Web services settings that the OTA Publisher application will use to push deployment packages to the deployment center.

Server Configuration > Properties > OTA Deployment Center

Download Interface
Enter a valid hostname or IP address, TCP port and URI reference pathname in the areas provided.

Address:

Port: [Reset to default](#)

URI ref: [Reset to default](#)

Web Services Interface
Enter a valid Web Services URI reference pathname. Provide a valid hostname or IP address and port if different from the Download Interface.

Use Different Address and Port

Address:

Port: [Reset to default](#)

URI ref: [Reset to default](#)

Logging
Enter how often the Afaria Server will poll the Deployment Center to retrieve status logs (minutes).

Download interface

Use the Download Interface area to configure how the planned Afaria Clients will communicate with the OTA Deployment Center Web server over the Internet.

- **Address.** The valid host name or IP address of your OTA Deployment Center Web server.
- **Port.** The port on which your deployment center Web server is running. Choose **Reset to default** to return the port number to its initial setting.
- **URI ref.** The alias portion of the full URL where the deployment center scripting information is located. Choose **Reset to default** to return the URI to its initial setting.

Web services interface

Use the Web Services Interface area to configure how the Afaria Server communicates with the OTA Deployment Center Web server using your intranet.

- **Use Different Address and Port.** Check this box to provide a different address and port other than the setting used for the Download Interface.
- **Address.** The valid host name or IP address for your Web services interface.
- **Port.** The port on which your Web services are running. Choose **Reset to default** to return the port number to its initial setting.
- **URI ref.** The alias portion of the full URL where your Web services are located. Choose **Reset to default** to return the port number to its initial setting.

Logging

Use the Logging spin box to determine how frequently—in minutes—the Afaria Server will poll the deployment center Web server to retrieve status logs for Afaria reports. Status logs are displayed in **Data views > Logs > Client deployment**, as well as **Data Views > Client deployment**.

Defining deployment protocol

Afaria Server default behavior is to use HTTP for OTA Client deployment downloads. The server stores the value in the Afaria database. You can change the value to change the default protocol.

- 1 Set the table's data value to the protocol you choose.
 - Afaria database table – A_Configuration_Property
 - DataName – DeploymentCenterDownloadProtocol
 - DataValue
 - http – Default. Afaria Server uses HTTP protocol for OTA Client deployment downloads.
 - https – Afaria Server uses HTTPS protocol for OTA Client deployment downloads.
 - No other value is supported.
- 2 Configure your download interface port value on Afaria Administrator's OTA Deployment Center page (**Server Configuration > Properties > OTA Deployment Center**) to an appropriate value for the protocol you specify in the table.

SMS Gateway

SMS, in this Afaria context, is the acronym for “Short Message Service”. It is a means of sending short messages to and from mobile phones. More specifically in Afaria, it is a means of sending SMS messages from the Afaria Server to mobile phones that may or may not be Afaria Clients.

Afaria uses the SMS gateway—for devices and Afaria Clients that support SMS messaging—to deliver outbound notifications, remote wipe commands, Open Mobile Alliance (OMA) provisioning and server notification messages, and any other Afaria communication that is addressed for SMS routing.



The SMS gateway requires installation prior to configuration. See “[SMS gateway installation](#)” on page 148.

Server Configuration > Properties > SMS Gateway

SMS Gateway Interface
Enter gateway configuration and character set.

Gateway port: 13000 Access phrase: zyytbd04 Character set: ASCII Status: []

Enable HTTPS Support

Cert file: certificates\Server\Server_through062010.cert Key file: certificates\Sever\Server_through062010.cert

SMSC Server Configuration

Create Delete

- SMPP Service
 - MySMPPService
- Modem
 - allcellular
 - mobiletoday

SMSC Server Configuration

* To add a new SMSC configuration, right click on an available type and select Create...

To successfully start the SMS gateway, you must first define the SMS Gateway Interface and at least one SMSC Server Configuration entity.

SMS Gateway Interface

Use the SMS Gateway Interface data elements to configure connectivity between the Afaria Server that is hosting the SMS gateway and the Afaria SMS gateway. In a farm environment, the Afaria Server is always the main server.

- **Port** – The first Afaria Server port number dedicated to SMS gateway communication. The server uses this port and the next two consecutive ports. For example, if you select port 3000, then the SMS gateway uses ports 3000, 3001, and 3002.
- **Access phrase** – The required phrase used for all communications from an Afaria Server to the SMS gateway. The SMS gateway ignores all communications requests that do not include the phrase.
- **Character set** – The character set that the SMS gateway uses to compose SMS messages. The appearance of the message at the Client is dependent upon the device's support for a given character set. Devices that only support ASCII but are sent a unicode-based message will display messages that are padded with extra characters.
- **Enable HTTPS Support** – Optional. Select the check box to enable HTTPS support for secure communications from the Afaria Server to the SMS gateway. See [“Tasks for successful HTTPS support”](#) .
- **Cert file** – The complete path and file name on the main Afaria server for the PEM-formatted certificate file. The SMS gateway uses the file to verify the identity of the Afaria Server.
- **Key file** – The complete path and file name on the main Afaria server for the PEM-formatted key file. The SMS gateway uses the file to verify the identity of the Afaria Server.

Tasks for successful HTTPS support

The Afaria Server runs on a Windows operating system. The SMS gateway, which runs on the Afaria Server, is encapsulated within an emulated Linux operating system environment. As two separate operating systems on the same server, HTTPS support requires installing a certificate that is known to both Windows and Linux.

The following steps summarize the procedure for obtaining and managing the required certificate.

- 1 Obtain a certificate and key that identify the Afaria Server in PEM format.
Ensure that the “common name” attribute on the certificate is the name of the Afaria Server, exactly as the name is defined in the “Gateway host” field on the SMS gateway's configuration page.
- 2 **Certificate for Windows** – Import the PEM-formatted certificate and its associated key as a visible Windows Trusted Root Certificate Authority. The Windows Trusted Root is accessible only to the Afaria Server.
- 3 **Certificate for Linux** – Complete the “Cert file” and “Key file” fields on the SMS Gateway Interface configuration page to point to the certificate and key files. The files must reside on the Afaria Server. The SMS gateway uses these references to access the certificates, as it cannot access certificates as imported into the Windows Trusted Root Certificate Authority.

SMS gateway status

Choose **Status** to open the SMS Gateway Server Status dialog box. The data provides information about the communication status with a selected SMSC entity.¹ The data is refreshed constantly.



An “X” icon next to an SMSC entity is an indication that the entity is offline.

SMS Gateway Server Status	
Server	
On Line	True
Queued	0
Sent	0
Received	0
Failed	0

Tmobile
Cingular

Name	Cingular
Type	Modem
On Line	False
Queued	0
Sent	0
Received	0
Failed	0

Close



The status dialog box reports only the status for message delivery from the SMS gateway to the SMSC entity you configured. The ultimate success or failure of delivery depends on additional components beyond the scope of your Afaria solution.

For example, the ability of the SMSC to receive and relay messages delivered by the SMS Gateway cannot be determined. Nor can the ability of devices to receive messages from wireless carriers be determined, such as when devices are powered off or outside of service areas. Although the send status may indicate success, you cannot assume a device has received a notification.

SMSC Server Configuration

Use the page's SMSC Server Configuration area to create, edit, and delete Short Message Service Center (SMSC) entities. You can create multiple SMSC entities, but Afaria uses only those that you enable.



Name and address format advisory!

- SMSC name – The name of your SMSC entity has a direct impact on how Afaria routes Afaria-initiated messages.
- SMSC address requirements – Your Short Message Service Center (SMSC) configuration entities may have address requirements for successful routing.

See [“Addresses and routing for Afaria messages”](#) on page 150 to understand address formatting and how Afaria routes SMS messages.

Each entity includes the following configuration items:

- Name – User-defined friendly name for your configuration.

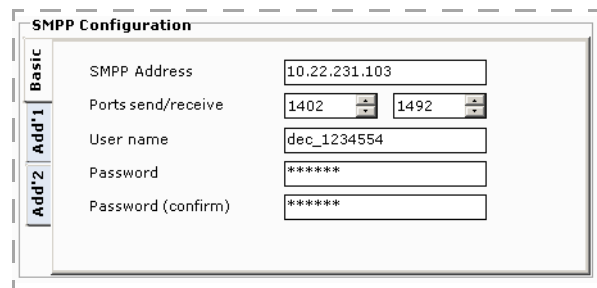
1. The “Received” data item is reserved for future use.

- Enabled – Select the check box to enable communications with this entity. Clear the check box to suspend communications but retain the configuration values.

SMPP Service

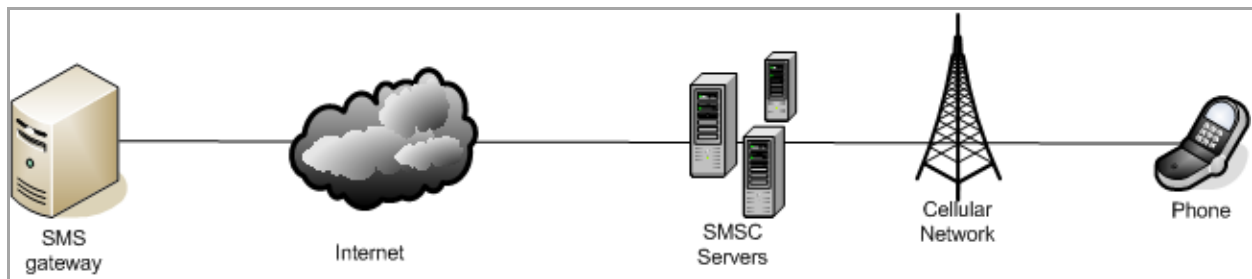
Short Message Peer-to-Peer (SMPP) is a protocol for delivering SMS messages directly to an SMSC or SMSC aggregator. SMPP services are typically carrier agnostic. Message routing from the SMS gateway is direct to the SMSC, rather than over a carrier network. As a result, an SMPP service can typically deliver most SMS messages to any carrier network.

The SMPP configuration data values are defined by your SMPP service provider, which may not require all of the available fields.



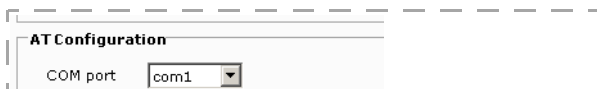
The screenshot shows the 'SMPP Configuration' dialog box with a 'Basic' tab selected. The fields are as follows:

Field	Value
SMPP Address	10.22.231.103
Ports send/receive	1402 / 1492
User name	dec_1234554
Password	*****
Password (confirm)	*****



Modem

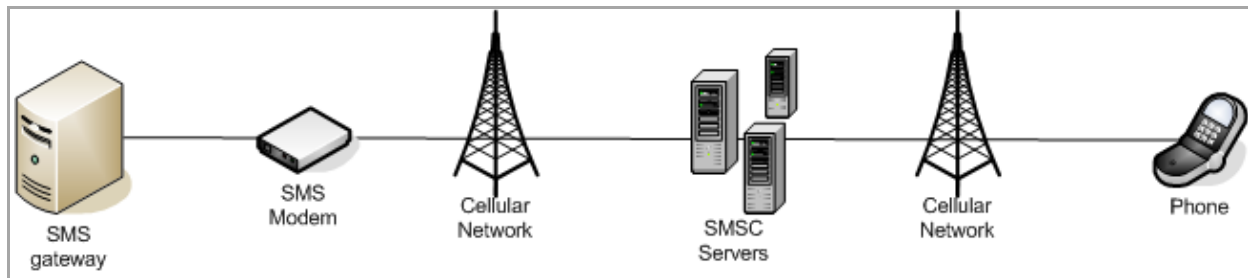
SMS modems are typically carrier specific, as each modem uses a carrier's Subscriber Identity Module (SIM) card. They use the associated carrier's network to deliver SMS messages to an SMSC; messages take an indirect path to the SMSC.



The screenshot shows the 'AT Configuration' dialog box with a 'COM port' dropdown menu set to 'com1'.

The modems can often support basic SMS message (example: text messages) delivery to different carrier networks. However, modems may be unable to deliver configuration messages (example: Afaria Open Mobile Alliance Client Provisioning (OMA CP) messages) to different carrier networks.

COM port – Afaria Server COM port for communicating with the modem. Ports 1–16 are valid for the SMS gateway operations.



SMS gateway installation

The Afaria solution leverages the Cygwin product's libraries and tools and other open source tools to implement its SMS gateway. The Cygwin product is a set of libraries and tools developed by Cygnus Solutions that creates a Unix-emulating environment on a Windows operating system.

Due to the nature of open source licensing practices, cited in the GNU General Public License, the libraries and tools cannot be distributed, installed, or licensed as part of a commercial product delivery. Therefore, it is your responsibility to obtain and install the required items on behalf of your organization to enable the SMS gateway operations in the Afaria solution.



SMS gateway operations use only some of the components of the Cygwin product. Therefore, the installation steps describe a manual process for installing only the component that the SMS gateway requires, rather than using Cygwin's installation program.

Install required components:

- 1 Visit the [Afaria third-party component dependency reference page](#), where you will find version information and download instructions for obtaining the Cygwin components.
- 2 Use a decompression utility to decompress the BZ2 download packages from within the `<download folder>` folder. For each installation package file with file extension "BZ2", the decompression yields one extracted file with file extension "tar".
- 3 Extract the decompressed packages into the same download folder. The file extraction creates the following folders:
 - `<download folder>\usr` – Folder contains additional, nested folders.
 - `<download folder>\etc` – Folder contents are not used for SMS gateway operations.
- 4 Modify the Afaria Server environment to include the required libraries and tools by either 1) including "`<download folder>\usr\bin`" in the default system path or by 2) copying the following "`<download folder>\usr\bin`" files into the Afaria folder "`<AfariaInstallation>\bin\SMSGateway`":
 - `cygcrypto-0.9.8.dll`
 - `cygiconv-2.dll`

- cygssl-0.9.8.dll
- cygwin1.dll
- cygxml2-2.dll
- cygz.dll

The default value for *<AfariaInstallation>* is "C:\Program Files\Afaria".

Use the Afaria Administrator Server configuration SMS gateway page after installing the required libraries and tools. See ["SMS Gateway Interface" on page 145](#).

Addresses and routing for Afaria messages

Both the Afaria SMS gateway and the SMTP server use addresses to attempt to deliver their respective Afaria-initiated messages to recipients. Depending upon the Afaria context for initiating the message, it may be an SMS message or e-mail message.

Addresses are used in multiple Afaria contexts, including but not limited to the following examples:

- Sending notification messages to devices for message broadcasts, provisioning, or Client deployment
- Sending alert notifications to an administrator contact
- Sending remote wipe commands to Afaria Clients

Address syntax

The address determines how Afaria routes the message. Format addresses with the following syntax:

<prefix>[<routing information>]

where < > encloses a parameter value and “[]” indicates an optional parameter



SMSC name and address format advisory!

- SMSC address requirements – Your Short Message Service Center (SMSC) configuration entities may have address requirements for successful routing. For example, a service provider or carrier modem may require that you format all mobile numbers in their respective international format and may stipulate that the leading “+” symbol is or is not part of the requirement. It is your responsibility to understand the requirements for your SMSC entities, and it is your responsibility to create your address entries appropriately.
- SMSC name – The name of your SMSC entity has a direct impact on how Afaria routes Afaria-initiated messages.

See [“SMSC Server Configuration” on page 146](#) for more information.

<i>Prefix</i>	<i>Routing information</i>	<i>Examples</i>	<i>Afaria routing logic</i>
<i>Prefix = <mobile number^a></i>			

<i>Prefix</i>	<i>Routing information</i>	<i>Examples</i>	<i>Afaria routing logic</i>
<prefix> +	<i>null</i>	= 5554122212 15554122212 +15554122212	IF any SMS gateway SMPP service is defined THEN send via SMPP service ELSE IF any SMS gateway entity is defined THEN send via SMS gateway entity ELSE discard message
<prefix> + <routing information>		= +15554122212@allcellular 5554122212@mobiletoday.com	IF <routing information> = an SMS gateway SMPP service name THEN send via SMPP service ELSE IF <routing information> = an SMS gateway modem name THEN send via modem IF any SMS gateway SMPP service is defined THEN send via SMPP service ELSE IF any SMS gateway entity is defined THEN send via SMS gateway entity ELSE send via SMTP server
<i>Prefix = <recipient identifier></i>			
<prefix> +	<i>null</i>	= john.doe jdoe	Invalid, discard message
<prefix> + <routing information>		= john.doe@mobiletoday.com jdoe@allcellular jdoe@mycompany.com	Send via SMTP server

a. A mobile number prefix must have a minimum of ten numeric characters, with or without a leading “+” character. Afaria discards messages with an invalid prefix.

Security

Use the Security property page to enable and disable for NT or LDAP user authentication, and set time out values for both authentication and assignments. If you are using LDAP for user authentication and assignments, you can enable and configure SSL for LDAP to increase security when you communicate with your Clients. You can also indicate whether new Clients are automatically approved. Approved Clients, when connected to the Afaria Server, are able to receive group profiles and system files. Finally, you can change your NT assignments and authentication domains or change your LDAP settings from this page.

Server Configuration > Properties > Security

Authentication

Enable authentication

Authentication timeout 0 Days 0 Hours 0 Minutes

Auto renew period 0 Days 0 Hours 0 Minutes

(must be equal to or smaller than Authentication Timeout)

Client approval

Automatically approve new Clients

Assignments

Assignments timeout 0 Days 0 Hours 0 Minutes

Domain

User assignments always allows local user groups. It allows domain user groups only if a valid NT domain was specified during the server installation.

NT default authentication None specified.

NT assignments domains None specified.

You must restart the service to use any new values.

Save Cancel

Example - NT Domain environment

The Security page contains the following fields and options:

- **Enable authentication.** When you select this option, you enable authentication for either NT or SSL communication between your server and Clients.
- **Authentication timeout and Auto renew period.** You can specify the amount of time a cookie is valid by setting an authentication time out value. You can also set a period of time during which a cookie nearing its expiration date will be automatically renewed if the Client user connects to the server during the specified time period.

For example, if you set the automatic time out period to 30 days and the auto renew period to two days, any users connecting to the server during the last two days of the automatic time out period will have their authentication cookie renewed for the next 30 days.

- **Client approval.** Select the **Automatically approve new Clients** option to automatically approve new Clients. Approved Clients, when connected to the Afaria Server, are able to receive group profiles and system files. The default setting for this option is to automatically approve new Clients. See [“How security works with Client approval” on page 157](#) for information on the Client approval setting.
- **Assignments timeout.** You can specify the amount of time the assignments cookie remains valid. If you add and remove users from domain groups, or organizational units or groups frequently, or if you regularly create and delete groups or organizational units, you may need a shorter timeout value.



A typical timeout value for both authentication and assignments is 30 days.

- **Domain.** If you are using NT for authentication and assignments, you can change the NT domain against which Client users are verified. If you did not specify any domain when you installed the server, it will automatically authenticate users against the local computer.



You can enter more than one domain for assignments. You must separate each assignments domain with a comma.

- **LDAP settings.** You can change the type of LDAP support used for authentication on your server. The server area displays the address for the LDAP server you chose during installation. The Search Root area displays the Search Root you specified. Both of these fields are read-only. You must re-install the server in order to change these values. You can select **Support OU membership** to support authentication against organizational units only, or you can select **Support OU and group membership** to support authentication against both organizational units and groups.
- **Enable SSL.** *This option only appears if you selected to use LDAP for authentication and assignments when you installed the server.* If you are using LDAP-based authentication, this option enables additional security between the Afaria Server and the LDAP server.



- For the greatest security level, you should enable both authentication and SSL. When you enable SSL from this page, you enable it only for LDAP-supported authentication and assignments.
- For information on enabling SSL-based encryption for Client communications, [“Client communication” on page 119](#).

How security works with NT

When you installed the server, you chose the type of authentication to enable. If you chose NT-domain based authentication, you may also have entered an NT domain. If you did not choose a domain, the server authenticates users against the local computer on which it resides. When Client users attempt to connect, the server uses the NT domain database you selected to verify the user before making channels available.



When you specify an NT domain, authentication is performed only against that NT domain user database.

NT authentication at the Client

When you've enabled authentication for a channel and a Client user tries to access that channel for the first time, the user must enter an ID and password. Once the server verifies the user's identity against the NT domain or local computer, the system generates a record—or "cookie"—of this authentication and passes it back to the Client.



You must disable the Guest account, or any authentication requests will pass.

The next time a Client user tries to access a channel on the same server, that server will locate the cookie at the Client and authenticate the user's identity, without prompting the user for ID and password.

The Client user must provide a user ID and password after:

- logging off Windows
- logging off the service
- logging off all servers
- restarting the computer
- the cookie exceeds the automatic timeout value.

Authenticating against different NT domains

Client users can override authentication for the default NT domain you specified during installation. This feature is particularly useful if you have many domains authenticating against a single server. Users can authenticate against any domain by entering the desired domain and a backslash before entering their user name. For example, when authenticating against the default domain, users enter their name and password like this:

User Name: John D

Password: xxxx

To authenticate against another domain, such as Marketing, users would enter their user name and password like this:

User Name: Marketing\John D

Password: xxxx

Allowing blank passwords

The Afaria solution supports allowing local and domain users to have blank passwords when making authentication requests. Observe the following item about using blank passwords in a Windows 2003 environment:

Windows 2003 Server – In order for a Windows 2003 Server to process requests that include blank passwords, you must disable the server's "Accounts: Limit local account use of blank passwords" local policy security option:

Administrative tools > Local Security Settings > Local Policies > Security Options

NT domains and assignments

You can assign specific NT domain user groups or local user groups to group profiles to control who views and accesses the profile's contents. Assignments work much like authentication. When Client users attempt to connect and receive their profiles, the server uses the NT domain you selected during installation to verify the user is a member of the assigned group before making profiles available.

NT Assignments at the Client

If you have not enabled authentication, assignments will use the currently logged on user account instead of prompting for user ID and password.

Once the server determines the NT group to which the user belongs, the server generates a record—or "cookie"—of this and passes the cookie back to the Client. Once the cookie exists at the Client, the system can quickly verify the user's group assignment and make the appropriate group profiles available to that user.

How security works with LDAP

If you are using LDAP-based authentication, the server authenticates users against the LDAP server you chose when you selected LDAP support. When Client users attempt to connect, the server uses the LDAP server you selected to verify the user before making group profiles available.

LDAP Authentication at the Client

When you've enabled authentication for a channel and a Client user tries to request that channel for the first time, the user must enter an ID and password. The server will use the User Name Attribute you selected for the user ID to verify the Client user. Once the server verifies the user's identity against the LDAP server, the system generates a record—or "cookie"—of this authentication and passes it back to the Client.

The next time a Client user tries to request a channel on the same server, that server will locate the cookie at the Client and authenticate the user's identity, without prompting the user for ID and password.

The Client user must provide a user ID and password after:

- logging off Windows
- logging off all servers
- restarting the computer
- the cookie exceeds the automatic timeout value

LDAP and assignments

You can assign specific LDAP directory organizational units and groups or local user groups to group profiles to control who receives the profiles. Assignments work much like authentication. When Client users attempt to connect, the server uses the LDAP server you selected during installation to verify the user is a member of the assigned organizational unit or group before making profiles available.

LDAP assignments at the Client

If you have not enabled authentication, assignments will use the currently logged on Windows user account instead of prompting for user ID and password.

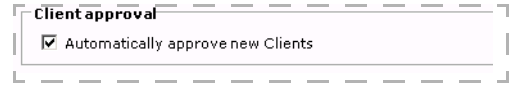
Once the server determines the LDAP directory organizational unit or group to which the user belongs, the server generates a record—or "cookie"—of this and passes the cookie back to the Client. Once this cookie exists at the Client, the system can quickly verify the user's organizational unit or group and make the appropriate group profiles available.

How SSL works with LDAP

When you enable SSL for LDAP, SSL works with LDAP to hide the user passwords that pass between the server and the LDAP server. Before you can enable SSL for LDAP, you must configure your LDAP server to communicate over an SSL port. See your LDAP server documentation for the steps to configure your LDAP server for SSL.

How security works with Client approval

The Client approval area on the Security page determines whether a new Client, when connected to the Afaria Server, is able to receive group profiles and system files. As a security measure, when the Client makes an initial connection with the Afaria Server, it can be marked as 'unapproved.' Unapproved Clients are not able to receive any profiles until the administrator 'approves' the Client. The default selection for this feature is **Automatically approve all new Clients** whenever the Afaria system is initially installed, re-installed, or upgraded. An administrator may disable or re-enable Client approval at any time.



Disabling Client approval automatically approves any previously unapproved Clients.

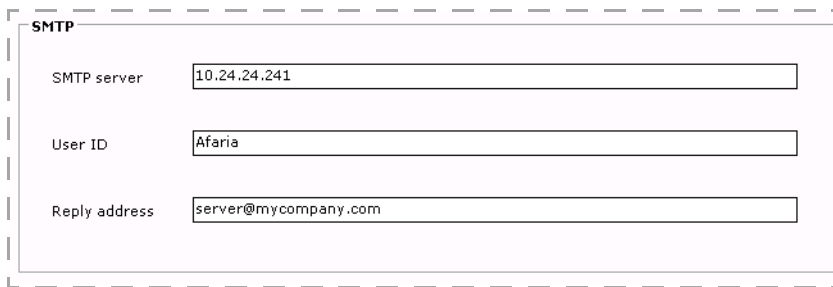
The Afaria administrator may use Data Views, Clients to approve or revoke one or multiple Clients. See ["Revoking and Approving Clients" on page 399](#) for information on revoking and approving Clients.

SMTP

Use the SMTP page to configure your SMTP server. The server can provide SMTP services for your Afaria solution for sending e-mail communications and e-mail-based Short Message Service (SMS) messages related to Afaria operations.

See [“Addresses and routing for Afaria messages” on page 150](#) to understand how Afaria routes messages.

Server Configuration > Properties > SMTP



The screenshot shows a configuration form titled "SMTP" with three input fields. The first field is labeled "SMTP server" and contains the value "10.24.24.241". The second field is labeled "User ID" and contains the value "Afaria". The third field is labeled "Reply address" and contains the value "server@mycompany.com".

The page contains the following fields:

- SMTP server – IP address or host name of the SMTP server that you use to send SMS messages.
- User ID – User ID for the SMTP server account that you use to send SMS messages.
- Reply address – Address to display on the SMS messages.

User defined fields

On the User-defined fields page, you can define or remove user-defined fields in your Afaria database. You can read from/write to these fields using the session worklist variables Set Database Field and Get Database Field. The Set Database Field variable associates (or writes) a value to the database field you create; the Get Database Field variable retrieves (or reads) the value associated with the field. These session events construct a SQL statement based on the input parameters you specify when you define these events.



- For detailed information on these events, see *Afaria Reference Manual | Components* appendix “Session Manager Events and Variables.”
- Any table that you build here you can view through Data views, Clients through the predefined view “User-defined data.” This view is dynamic according to any changes made to user-defined fields. For more information, [“Managing Client Data” on page 395](#).
- Multitenant users – User defined fields are global, available for all tenants.

Server Configuration > Properties > User Defined Fields

User defined fields

To add new fields in your database tables related to the A_CLIENT table, click 'Add Field'. You can read from and write to these fields using session worklist variables.

[Add field](#) Delete selected field

Field	Type	Length (bytes)
My field 1	INTEGER	4
My field 2	DATETIME	8
My field 3	FLOAT	8
My field 4	VARCHAR	7

Save Cancel

The User-defined fields page contains the following fields:

- **User-defined fields list box.** This contains the list of all user-defined fields, sorted alphabetically.
- **Add field.** When you click this link, the Add field dialog box appears.

From this dialog box, you type a name for the user-defined field and select the field type: Integer, Float (a floating point decimal), Date/Time, Varchar (a variable length string)



The Varchar field length is limited to 255 characters, as the worklist only supports strings of this length.

Delete selected field. You can select any user-defined field from the list and then click this option to delete the field from both the list and the database.



If you are using Oracle for your Afaria database, the Delete selected field option is unavailable; Oracle does not support this action.

Add field

Instructions

To create a field name containing spaces or other "special" characters, enclose the field name in double quotation marks in the Field Name box:

"My field 1" (correct)

My field 1 (incorrect - will likely fail)

Note that field names must comply with the database's naming rules for table column names. These rules vary from one database backend to another.

Please consult with your database administrator if you have trouble creating a field.

Field name:

Field type:

OK Cancel

Outbound notification

On the Outbound notification page, you can set the “flood control” level to prevent the Afaria Server from being overwhelmed with incoming sessions. The Afaria Server also has “notification retries” which can be set to retry notifications to Clients who still have channels that they have not run.

Flood control

Set the following values to control the number of Client notifications sent during a given time period. These values prevent too many Clients from connecting to the Server at once.

If you select zero, the Server will ignore the setting.

High water	<input type="text" value="500"/>
Low water	<input type="text" value="450"/>
Maximum per time period	<input type="text" value="500"/>
Time period in seconds	<input type="text" value="600"/>
Max Simultaneous Notifications	<input type="text" value="20"/>

[Reset to defaults](#)

Notification Retries

Enable Notification Retries

Set the following values to control how much time must have elapsed since the last notification on a given client in order to re-notify it, and the maximum number of retries allowed depending on the notification type.


Retry Wait Time

days	hours	minutes
<input type="text" value="1"/>	<input type="text" value="4"/>	<input type="text" value="20"/>

Maximum SMS Retries

Maximum IP Retries

[Reset to defaults](#)

 You must restart the service to use any new values.

Flood control

Using flood control, for example, if you send a notification for a Client group with 5,000 members, you can specify that the server send ten notifications every thirty seconds until it reaches a “high water” level of 200 connected sessions. Once this happens, the server will stop notifying Clients until the number drops below the “low water” level of 125, at which point it will resume sending ten notifications every thirty seconds.

Flood control includes the following data elements:

- High water – Notifications from the server will stop when the number of active sessions on the Afaria Server reaches this number. To ignore this setting entirely, set the value at zero (0).
- Low water – Notifications will resume when the number of active sessions drops to this number. To ignore this setting entirely, you can set the value at zero (0).
- Maximum per time period – This value sets the number of sessions that can occur within the time period you specify in the Time period in seconds spin box. To ignore this setting entirely, you can set the value at zero (0); if you set this value to zero, you must also set the Time period in seconds value to zero (0).
- Time period in seconds – This value defines the time period in seconds for the Maximum per time period value you set. To ignore this setting entirely, you can set the value at zero (0); if you set this value to zero, you must also set the Maximum per time period value to zero (0).

- **Max. Simultaneous Notifications** – This value defines the number of notifications to group together at one time. Grouping notifications provides efficiency gains in the send-and-wait process. However, defining your groups very large may cause too many Clients to try to connect at one time. To ignore this setting entirely, you can set the value at zero (0).

You can choose **Reset to defaults** at any time to return to the default values for flood control.



If you are using over-the-air (OTA) deployments and you are not licensed for Outbound, the Max. Simultaneous Notifications data element defaults to 20 and **you are not able** to modify this setting.

If you are licensed for Outbound, the Max. Simultaneous Notifications data element defaults to 20, and **you are able** to modify this setting.

Notification retries

Using notification retries, for example, if you send a notification request to run a channel and that a Client is unable to connect to the Afaria Server, you can specify a retry wait time of 20 minutes. The server will send a notification to the Client every 20 minutes until it has sent 21 notifications (one request and 20 retries), or whatever you set as the maximum number of IP retries.

Notification retries includes the following data elements:

- **Retry Wait Time** – This value sets the amount of time in days, hours, and minutes, to wait after a notification before the Client is re-notified. The maximum values for the days, hours and minutes spin boxes are 30, 23, and 59 respectively. To ignore these settings entirely, set the values to zero (0).
- **Maximum SMS Retries** – This value sets the number of Short Message Service (SMS) retries that can occur in the time period you specify in the days, hours, and minutes spin boxes. The maximum value is 100. If the maximum number of SMS retries is met, and a new notification request is made, the count will restart. To ignore this setting entirely, set the value to zero (0).
- **Maximum IP Retries** – This value sets the number of IP retries that can occur in the time period you specify in the days, hours, and minutes spin boxes. The maximum value is 100. If the maximum number of IP retries is met, and a new notification request is made, the count will restart. To ignore this setting entirely, set the value to (0).

The number of IP notification retries selected from the **Notification retries** section of the **Outbound Notifications** window apply to each IP Client connected to your servers. Therefore, IP notification retries will be sent to more than one location for all Windows Clients based on your notification flow control parameters.

You can click **Reset to defaults** at any time to return to the default values for notification retries.

Relay server



- Use of 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. Afaria also supports making direct connections to the Afaria Server.
- See *Installing Afaria* to learn about installing the relay server and creating its configuration file.
- See [“About the relay server” on page 21](#) to learn more about the relay server, including a diagram and discussion of its components.

You use the Relay server page to define settings for relay server's outbound enabler service. The outbound enabler is the relay server's agent on the Afaria Server. It is responsible for initiating an outbound connection with the relay server, while sustaining a connection with the Afaria Server. The settings define communications with your relay server and the Afaria Server.

All relay server communication must use HTTP or HTTPS protocol. Therefore, you must also configure the Afaria Server and Clients to use HTTP or HTTPS. See [“Client communication” on page 119](#).

Server Configuration > Properties > Relay Server

Outbound enabler

Start the outbound enabler with the Afaria service.

Farm ID:

Farm token:

Server address:

Server port:

RS address:

RS port:

RS URL suffix:

Maximum restarts:

Client URL prefix:

Use HTTPS

Certificate path:

The Relay server page contains the following fields, several of which must match corresponding values in the relay server's configuration file:

- **Start the outbound enabler.** Selecting this check box applies an automatic startup attribute to the outbound enabler service. Afaria logging captures the outbound enabler's restart and failure events.
- **Farm ID and Farm token.** A pair of case-sensitive, ASCII text strings that your relay server uses to direct incoming Client communication to your Afaria Server, either a standalone

server or server farm. The combination of the strings must be unique for a given Afaria instance.

- **Farm ID** – Value must match the corresponding value in your relay server's configuration file and in your Client Afaria configuration settings. The value you use seeds new Client packages that you create using the Create Client Installation program.
- **Farm token** – Value must match the corresponding value in your relay server's configuration file.
- **Server address and Server port.** The Afaria Server IP address or "localhost" and HTTP port that the Afaria Server is using for communications. In a server farm environment, you are required to enable HTTP on each Afaria Server in the farm.
- **RS address and RS port.** The relay server IP address or fully-qualified domain name and port that the outbound enabler service uses to connect to the relay server.
- **RS URL suffix.** Text string used as an IIS parameter for invoking the relay server's Afaria Server Web services it requires, as per the relay server installation instructions for creating the IIS application pool.
- **Maximum restarts.** The maximum number of times the outbound enabler attempts to start if it stops unexpectedly.
- **Client URL prefix.** Text string used as an IIS parameter for invoking the relay server's Afaria Client Web services it requires, as per the relay server installation instructions for creating the IIS application pool. This value is also required as a configuration value on Afaria Clients. The value you use seeds new Client packages that you create using the Create Client Installation program.
- **Use HTTPS.** Select the check box to enable the outbound enabler to communicate via SSL to the relay server.
- **Certificate path.** The path and file name on the Afaria Server for the relay server's certificate file. The certificate contains the relay server's identity and public key.

About using SSL with the relay server

Client-to-relay-server security – To configure the relay server to use SSL, you must install a trusted certificate on the server that is running the relay server's Microsoft Internet Information Services (IIS) Server and the relay server engine, RSHOST.EXE. You can configure Afaria Clients to connect securely using the relay server address and HTTPS protocol after you have the certificate installed. Connecting to the relay server with SSL ensures that all the traffic from the Client to the relay server is encrypted. If your Afaria Server and relay server are behind the same firewall, this configuration is all you need to secure your data.



The Symbian OS security environment does not allow devices to authenticate against self-signed certificates. Therefore, Afaria Symbian Clients do not support connecting to a relay server that uses self-signed certificates.

Relay-server-to-Afaria-Server security – Encrypting traffic between the relay server and the Afaria Server requires that you export the relay server's public key and copy the resulting file to the Afaria Server, then use the Afaria Administrator's Relay server page to enable HTTPS and

specify the location of the public key file. Encrypted traffic begins after you restart the Afaria Server.

Relay-server-related logging

Relay-server-related logging occurs both on the Afaria Server and the relay server.

- Afaria-side logging – Afaria logging captures the outbound enabler’s restart attempt events. Afaria logging does not capture relay server start events when started by the Afaria service, as occurs when the “**Start the outbound enabler**” setting is selected.
- Relay-server-side logging – Relay server logging captures events while rshost.exe is active. When started using the relay server’s configuration file setting for auto start, the log is stored in the following relay server path:

```
<tmpdir>\ias_relay_server_host.log
```

Where the value of <tmpdir> is populated with the first-available environmental variable, according to the following search order: SATMP, TMP, TMPDIR, TEMP.

To retrieve logging from the relay server to the Afaria Server:

The relay server log captures connections from the Afaria Server to the relay server and successful Client connections. The log does not capture unsuccessful Client connections.

- 1 Clear the “**Start the outbound enabler**” checkbox to prevent the outbound enabler from starting during Afaria’s next restart.
- 2 Restart the Afaria service.
- 3 Restart the outbound enabler using the following single, continuous command on the Afaria Server’s \bin\RSOutboundEnabler\ command line:

```
rsoe.exe -id <AfariaServerID> -f <FarmID> -t <Farm token> -cs  
"host=localhost;port=<AfariaHTTPPort>;" -cr  
"host=<RelayServerIP>;port=<RelayServerHTTPPort>;url_suffix=<RsURLSuffix>;url_prefix=<Client  
URLPrefix>" -v <LogVerbosity> -o <LogOutputPathFile>
```

Where:

- <AfariaServerID> – The Afaria Server ID value. The ID value is defined in the Afaria Server’s registry key HKLM\Software\Afaria\Afaria\Server\TransmitterId.
- <FarmID> – Farm ID, as stored on the Relay Server configuration page.
- <Farm token> – Farm token, as stored on the Relay Server configuration page.
- <AfariaHTTPPort> – Afaria’s HTTP port, as stored on the Client Communications configuration page.
- <RelayServerIP> – Relay server IP address.
- <RelayServerHTTPPort> – Relay server HTTP port.
- <RsURLSuffix> – RS URL Suffix, as stored on the Relay Server configuration page.

- <ClientURLPrefix> – Client URL Prefix, as stored on the Relay Server configuration page.
- <LogVerbosity> – Controls the level of logging. Logs always include errors. Logs always include warning for levels 1-5.
 - 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
- <LogOutputPathFile> – Afaria Server path and file name for the log file.

You may use command “rsoe.exe” without any parameters or options to open an Outbound Enabler window and view a usage example with an options list.

Example relay server log retrieval

The following sample writes the log file to c:\outbound.log on the Afaria Server. The sample is not based on the data depicted in the Relay Server configuration page screen example.

```
rsoe.exe -id got -f AfariaFarm -t Token_00 -cs "host=localhost;port=80;" -cr  
"host=10.14.229.21;port=80;url_suffix=/ias_relay_server/server/rs_server.dll;url_prefix=/  
ias_relay_server/client/rs_client.dll" -v 5 -o c:\outbound.log -af
```

Restarting the relay server

Restart the relay server any time you change the relay server configuration file or want to restart the relay server engine.

You can issue commands to restart 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:

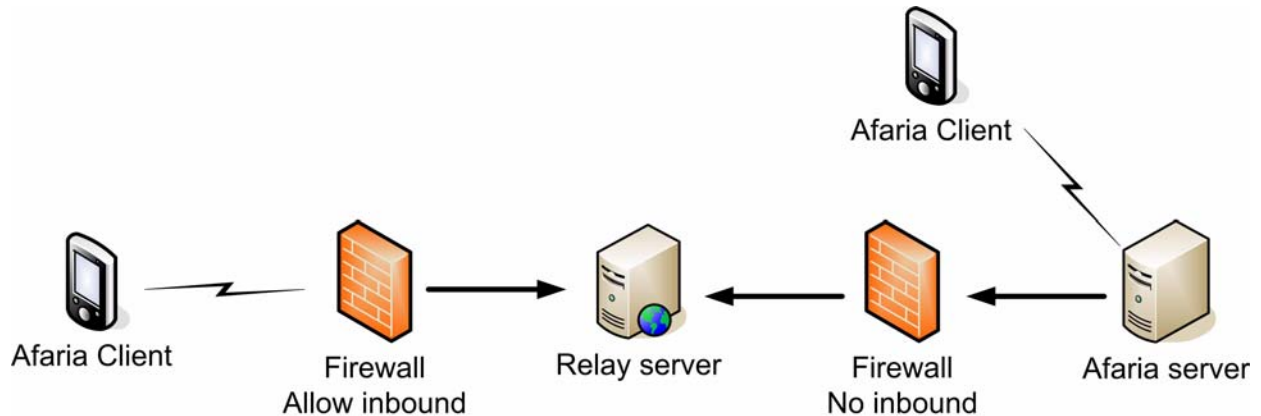
```
CD \inetpub\wwwroot\ias_relay_server  
rshost.exe -u -qc -f rs.config
```

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

Bypassing the relay server

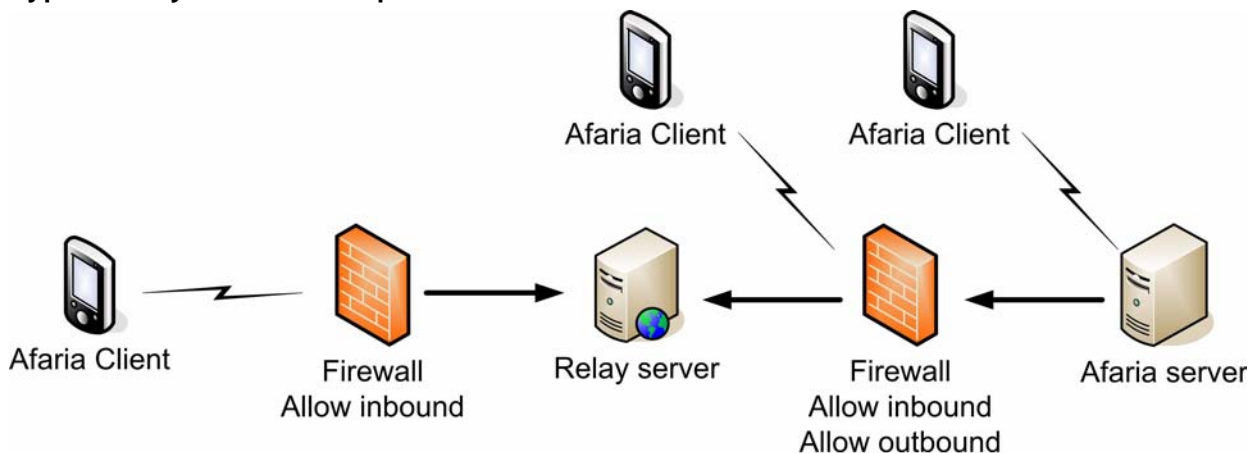
Even after your relay server is operational, the Afaria Server continues to support direct Client connections. If it is appropriate for your environment, you may allow Clients to continue to connect to the Afaria Server directly, bypassing the relay server altogether.

Bypass relay server – Sample 1



As the diagram above illustrates, if you have Afaria Clients that are inside your organization's firewall and want to connect, you can allow these Clients to make direct connections with the Afaria Server using any of Afaria's supported session protocols. These connections do not need to pass through the firewall, so the firewall can support higher security.

Bypass relay server – Sample 2



As the diagram above illustrates, if you have Afaria Clients that are outside your organization's firewall and want to connect, you can allow these Clients to make direct

connections with the Afaria Server using any of Afaria's supported session protocols as long as your firewall permits the traffic.

AV/Firewall

Use the server component configuration properties to determine the disposition of new client files or pattern files and to identify the date of the last update.

When you receive new client files, select one of the following:

- Hold for administrator approval – Wait for approval of the administrator.
- Automatically send to client on next connection – Distribute new client files when the client and server are connected.

When you receive new pattern files that contain the most current virus defects list, select one of the following:

- Hold for administrator approval – Wait for approval of the administrator.
- Automatically send to client on next connection – Distribute new pattern files when the client and server are connected.

Server Configuration > Properties > AV/Firewall

Update server address:
[AntiVirus update schedule](#)

When new client files received

Hold for administrator approval

Last Update 7/27/2009 (in use)

Automatically send to client on next connection

When new pattern file received

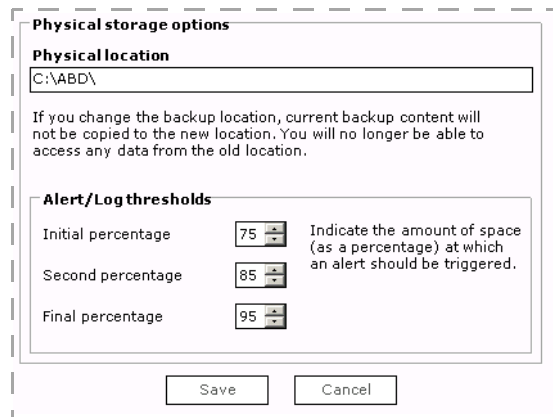
Hold for administrator approval

Last Update 4/13/2009 (in use)

Automatically send to client on next connection

Backup Manager

You use the Backup Manager page to change the default location for backed-up information and to set space-usage thresholds for backed-up items.



The screenshot shows a dialog box titled "Physical storage options". It has two main sections: "Physical location" and "Alert/Log thresholds".

Physical location: A text box contains "C:\ABD\". Below it is a warning: "If you change the backup location, current backup content will not be copied to the new location. You will no longer be able to access any data from the old location."

Alert/Log thresholds: Three spin buttons are shown: "Initial percentage" (75), "Second percentage" (85), and "Final percentage" (95). To the right of these buttons is a note: "Indicate the amount of space (as a percentage) at which an alert should be triggered."

At the bottom of the dialog are "Save" and "Cancel" buttons.

The Backup Manager page contains the following fields:

- **Physical location.** You can change the location specified during installation to a new location for storing backed-up information by typing the new path and the directory name in this field.



For a Backup channel to write to a new location, you must have an account at the new location equal to the account which the server service is logged on. Changing the backup location to a UNC name or a mapped drive will fail.



When you change a backup location, all previously backed-up content becomes orphaned and is unavailable for restores or for administrative purposes. You can avoid having orphaned data by deleting the Clients from the view before changing the physical backup location. If you change the backup location *without* deleting the Clients, you can manually clean up the orphaned data at the previous backup location in Windows Explorer.

- **Alert/Log thresholds.** Use the spin buttons to set threshold percentages when the space usage at the backup location exceeds a specified percentage. When the backed-up files consume the available disk space, Message log entries and alerts are generated.

Document Manager

You use the Document Manager page to apply certain default settings to your Document Manager channels for Channel Viewer users. For example, if you create different channels that all use the same Client media as the file source, you can specify new channels use the same Client media by default. Until you change the default settings, every new Document Manager channel you create is configured this way.

The screenshot shows a configuration window for the Document Manager Channel Editor. It is divided into two main sections: "Editor options" and "Client media".

Editor options:

- A checkbox labeled "Hide dependent items in the tree" is currently unchecked.
- A text input field labeled "Initial directory for selecting file" contains the text "DefaultMediaLabel".
- A blue "Browse" link is located below the text input field.

Client media:

- A checkbox labeled "Allow new channels to use Client media as source location by default" is currently unchecked.
- Two radio buttons are present: "CD" (selected) and "Floppy".
- A text input field labeled "Media label" contains the text "DefaultMediaLabel".
- A text input field labeled "Location of client media" is empty.
- A blue "Browse" link is located below the "Location of client media" field.

At the bottom of the window, there are two buttons: "Save" and "Cancel".

The Document Manager page contains the following fields:

- **Hide dependent items in the tree.** This option prevents Document Manager from displaying dependent files beneath the main files in the tree directory on the Documents property page in the Document Manager Channel Editor. Dependent files still appear as channel members and are still listed in the Dependent Files list box in the right pane of the Documents property page in the Document Manager Channel Editor.
- **Initial directory for selecting file.** In this area, you enter the path you want to use as the default path whenever you click Browse in the Document Manager Channel Editor.
- **Allow new channels to use Client media as a source location by default.** This option allows you to configure the Document Manager Channel Editor so that each time you create a new Document Manager channel, it is ready to use Client media as a file source.
- **Media label.** In this area you can enter a name to use for all Client media. This name will appear to Channel Viewer users when they attempt to access a media-based file.
- **Location of Client media.** In this area, you can enter the network path you want to use as the default for all media-based files, or you can click **Browse** to navigate to the location.

Exchange ActiveSync policy



The Exchange ActiveSync policy page is part of the implementation for the Afaria Access Control for Microsoft Exchange feature in your Afaria solution.

This feature requires Data Security Manager licensing.

About the Afaria Access Control for Microsoft Exchange feature

Afaria Access Control for Microsoft Exchange lets you add a layer of protection to your Exchange Server. The feature filters Exchange ActiveSync device synchronization requests by either 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 filtering is specific to Exchange ActiveSync device synchronization requests. The filter does not prevent device synchronization requests initiated by alternate means, such as the following methods:

- Web browser Client
- ActiveSync installed on a companion PC
- iAnywhere Mobile Office Client



- The default synchronization policy settings at installation time blocks all synchronization requests from Afaria Clients until you define an appropriate policy for your organization and have Clients run Afaria sessions.
- Exchange ActiveSync Clients that make synchronization requests after the filter is installed but before they connect to the Afaria Server are blocked from synchronizing. Therefore, establish your organization's default Exchange ActiveSync policy setting before Clients connect and before the filter becomes active. See "[Setting the default synchronization policy and time frame](#)" on page 175.

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

- 1 Use the 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 Internet Information Services (IIS) Server. The filter monitors all Exchange ActiveSync synchronization requests on behalf of Afaria.

IIS Server ISAPI filter

This Afaria feature requires that you install and register a new Afaria ISAPI filter with its supporting files onto the Internet Information Services (IIS) Server that serves your Exchange Server. ISAPI filters are developed as DLL files to modify and enhance the functionality provided by IIS. The filter monitors all Exchange ActiveSync synchronization requests on behalf of Afaria. The filter discards any request that does not meet your Afaria-defined policy for valid ActiveSync requests.

The filter is easy to install and is completely removable. See [“The ISAPI filter” on page 177](#).

Exchange Server

This Afaria feature does not require you to update or install anything on your Exchange Server. The Exchange Server gains the extra layer of protection for Exchange ActiveSync processing that this feature offers by receiving and servicing only those Exchange ActiveSync synchronization requests that are delivered by the IIS Server, subject to the Afaria ISAPI filter.

The Exchange ActiveSync policy configuration page

Use the Exchange ActiveSync policy page to define a synchronization policy for your enterprise's Windows Mobile devices that use Exchange ActiveSync to synchronize with your organization's Exchange Server. The Client list may include the following types of members:

- Afaria Clients that have connected and received a policy assignment.
- Any “white list” devices that you add to the list. These devices are not Afaria Clients and therefore do not connect to the Afaria Server but are subject to the policy you assign.

Use this page to establish a default policy setting applied to connecting Afaria Clients that do not yet have a policy assignment. You can also change the policy setting for one or more individual Clients that already have a policy assignment.

Server Configuration > Properties > Exchange ActiveSync Policy

Exchange ActiveSync policy

User name	SyncPolicy	Afaria	Data Security Ma...	Exchange device...
sales\ajjkin	0			9JF9034J4R034...
sales\ajk	1			9C9F9CJ9J3H3H...
shpmnt\vkroq	1			0FMWEOWERNO...

SyncPolicy key

- 0 Always block
- 1 Always allow
- 2 Allow by time frame
- 3 Allow by time frame & Data Security Man

Default policy

Select the default policy for devices Afaria adds to the policy.

0 Always block

Devices: 3/3

Get next Records

Device list

Time frame

Define the connection frequency requirement for Afaria Clients.

Days Hours

The device list

The device list displays your Afaria Clients and white list devices that currently have a synchronization policy assignment. The Afaria Server populates this list with Afaria Clients after it assigns a synchronization policy to a connecting Client. White list devices populate the list as you add them. Therefore, the list starts empty and grows as each Afaria Windows Mobile Client connects and receives its synchronization policy assignment and you manually add devices.

The list includes the following information as last retrieved from Clients and devices:

- User name – ActiveSync domain and user name used to synchronize with the Exchange Server.
- SyncPolicy – The Client's current policy assignment, as defined by the SyncPolicy key.
- Afaria – Indicates whether the Afaria Client is installed on the device. A blank value indicates that the Client is not installed.
- Data Security Manager – Indicates whether the Afaria Data Security Manager is installed on the Client. A blank value indicates that the Client is not installed.

- Exchange device ID – Exchange-defined identifier for the synchronizing device.



Afaria Clients

The synchronization policy is always executed based on the current Afaria-defined SyncPolicy value and the Client's last-known state. Changes in device state that occur between Afaria connections are not known by Afaria Server until the Client makes a subsequent connection.

For example, installing or uninstalling Data Security Manager on an Afaria Client is not known to the Afaria Server until the device connects after the process is complete. Therefore, synchronization requests made between the time of change and the subsequent connection are honored or blocked according to the last known Client state.

Synchronization policies defined

Afaria supports the following synchronization policies:

- Always block – Block Client's or device's synchronization requests at all times.
- Always allow – Allow Client's or device's synchronization requests at all times.
- Allow by time frame – (Afaria Clients only) Allow Client's synchronization requests if the Client's last Afaria connection occurred within the defined time frame.
- Allow by time frame & Data Security Manager – (Afaria Clients only) Allow Client's synchronization requests if the Client has the Afaria Data Security Manager Client installed and the Client's last Afaria connection occurred within the defined time frame.

The “Time frame” value is relevant only for the policies that state “time frame”. The value defines the frequency requirement for an Afaria Client to connect to the Afaria Server in order to be allowed to continue using Exchange ActiveSync for synchronization. Clients that are blocked based on time frame can connect to the Afaria Server and then issue a new synchronization request. The time frame setting is global for any Client that at any time uses a time frame policy; changing the value impacts all Clients that already have a time frame policy and all Clients that you subsequently assign a time frame policy.

Setting the default synchronization policy and time frame



The default synchronization policy setting is valid only for Afaria Clients.

The default policy is applied to connecting Afaria Clients that do not yet have a policy assignment. Changing the default synchronization policy impacts only additional connecting Clients; Afaria does not retroactively apply the changed default to previously-connected Clients.

- 1 Select a value from the “Default policy” list to establish the default synchronization policy for Clients.

- 2 Set the “Time frame” value, even if your default synchronization policy does not include consideration for time frame. This setting is global for any Client that at any time uses a time frame policy.

Adding white list devices to the device list

White list devices are supported Exchange ActiveSync devices that are not Afaria Clients but are devices that you control with your Afaria Exchange ActiveSync policy by adding them to the device list.

- 1 Choose **Add Device** to open the Add Device dialog box.
- 2 Complete the following information for the device:
 - Exchange device ID – Exchange-defined identifier for the synchronizing device.



The Exchange device ID value is the “DeviceID” value stored in the device's registry. You can obtain the value from a device if it has already connected to the Exchange's IIS Server. Afaria cannot retrieve the value for you because the device is not an Afaria Client. You can use your own method to retrieve the value or use one of the following methods:

- Use a device utility to read the value.
 - Use your Exchange Server ActiveSync Web Administration tool (browser address: <http://<YourExchangeServer>/mobileadmin>, this is the default location) to run a query to retrieve the Exchange device ID value. Choose the Remote Device Wipe menu option and query for the user of interest. The query returns information about the devices associated with the user. Copy the value from the Device ID column and exit the page without initiating any further action.
- User name – The user node of your fully-qualified ActiveSync user name used to synchronize with the Exchange Server.
 - Domain – The domain node of your fully-qualified ActiveSync user name used to synchronize with the Exchange Server.
- 3 Choose **OK**.

Removing devices from the device list

You can remove Afaria Clients or white list devices from the device list by selecting one or more devices and choosing **Remove Device**.

Changing the synchronization policy for one or more devices

- 1 Select one or more Clients or white list devices on the device list.

- 2 Press Enter to open the SyncPolicy dialog box.

Including one or more white list devices in your selection results in the user interface limiting the policy choices to only those selections that are valid for white list devices.

- 3 Select policy and choose **OK**.

The ISAPI filter



Installing this filter blocks all synchronization requests from devices that are not Afaria Clients.

Supply information to your Exchange Server's IIS Server administrator to provide guidance for installing the filter and setting the IIS authentication method.

ISAPI filter – Installing the IIS Server's ISAPI filter

Deliver the installation wizard and the following information to the IIS Server administrator.

- ISAPI filter installation folder as provided on the Afaria product image. The folder contains the installation wizard.
- Afaria database server name.
- Afaria database name.
- Read access to the Afaria database.

The following instructions install and register the Afaria ISAPI filter and its supporting files on the Exchange Server's Internet Information Services (IIS) Server.

- 1 Store the ISAPI filter component folder in a temporary directory on the IIS Server's local drive.
- 2 Open the folder and run the setup executable to open the Afaria ISAPI Filter Setup program wizard.
- 3 Use the Afaria database values to respond to Afaria database prompts.
- 4 Follow the installation wizard until the installation is complete.
- 5 To verify the filter properties, open the IIS Server's **Default Web Site > Properties > ISAPI Filters** tab. Look for filter name "XSISAPI.DLL" on the list.

ISAPI filter – Set authentication methods

The filter implementation requires the following specific security settings to operate successfully.

<MicrosoftServerActiveSync> > Properties > Directory Security > Edit (Authentication and access control):

- Enable anonymous access – Disable
- Integrated Windows Authentication – Disable
- Basic authentication – Enable

See Microsoft references for detailed information about IIS Web Site authentication methods.

ISAPI filter – New file list

Installing the Afaria ISAPI filter adds the following files to your IIS Server.

<IIS_InstallDir>

AfariaISAPIFilterUninstall.ini

XSISAPI.dll

<IIS_InstallDir>\bin

InstUtil.dll

End user notification

Notify your Afaria Client and white list device users about their synchronization policy assignment. It is your responsibility to establish an appropriate understanding about how to comply with the policy requirements and establish expectations about a device's synchronization denied behavior and corrective action if they fall out of compliance.

Manager for SMS

You use the SMS page to specify settings for importing Microsoft Systems Management Server (SMS) packages into the server. When you import SMS packages, Software Manager collects all necessary information to create an equivalent Software Manager channel. Once a package has been imported into the server, you can view its contents, unpublish and publish it, make a working copy, and delete the imported package. Additionally, you can synchronize the imported package with its original SMS package.



Every SMS package you import into the server becomes a Software Manager channel for Windows Client types, regardless of the files included in the package.

SMS servers

[Add server...](#)

Edit server...

Delete server...

Channel import

Automatically import channels

Import now

Channel settings

Assign automatically Publish

Encrypt AutoSubscribe

Authenticate Assignments...

Check files options

Always check file

Only check file when package is updated

Send file options

Send file when server file is newer

Send when server file is different

Package settings

Synchronize SMS package settings Difference all files

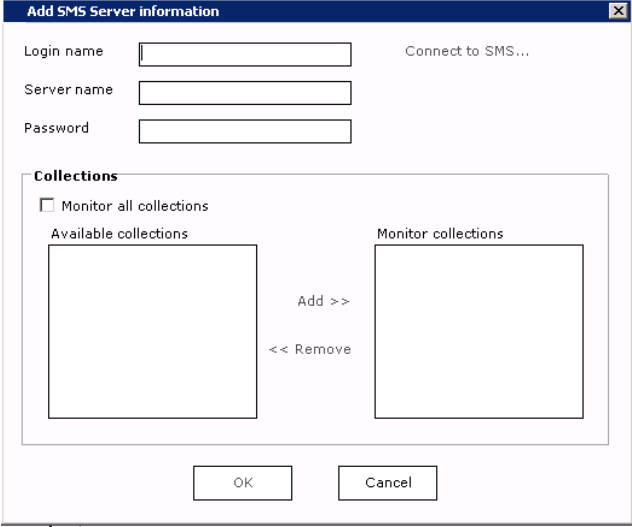
Start installation automatically on the client Local install

Save Cancel

SMS Servers

Use the features in this area to add, edit, or delete SMS servers from which you want to import packages. The Windows account that you use to connect to the SMS server should belong to the same domain as the SMS server itself. At a minimum, the account should have Read permissions on Advertisements, Packages, and Collections on the SMS server. If you are working with multiple SMS sites, you can only connect to a “primary” site, not to a “secondary” site. However, the primary site can be either a “parent” or “child.” When you click **Add**, the Add SMS Server information dialog box appears.

The Add dialog box contains the following fields and options:



- **Login name.** The Windows account that identifies you as a user and gives you access to the SMS site database.
- **Server name.** The name of the SMS server that contains the Collection you want to monitor. The name should contain the domain name as well as the machine name (i.e., hq\sms1).
- **Password.** The password for the login account.
- **Connect to SMS** This link connects you to the SMS server you entered in the server name field.



If you encounter problems connecting to the SMS server, verify that there's a trusted domain relationship between the server domain and the SMS server domain where the SMS database files reside. If these servers are on different domains, you must establish a two-way trust between the two domains in order to connect to the SMS server. If you configure both machines to use a single domain and have the Afaria service account as the domain administrator, you can insure that sufficient privileges are granted.

- **Collections.** The Available collections list box displays collections associated to software packages that you want to import.
 - *Monitor all collections.* You can select the Monitor all selections check box to monitor all the collections in the Available collections list box. If you select this option, the server will only import software packages that are assigned to SMS collections that contain Windows Clients.



If you select the Monitor all collections option, inventory data must be forwarded to SMS.

- **Monitor specific collections.** You select a collection from the list and click **Add** to add it to the list of collections to monitor. If you select specific collections for the server to monitor, it will import every software package assigned to those collections, regardless of the members of the collections.



You can only import software packages that are assigned to a collection.

Channel import

When you import SMS packages, Software Manager collects all of the information necessary to create an equivalent Software Manager channel. Once a package has been imported, you can view its contents, unpublish and then publish it, make a working copy, and delete the imported package. Additionally, you can synchronize the imported package with its original SMS package.

Regardless of the method you choose, before you import packages ensure that the Afaria Service Account has all of the necessary rights and permissions.

Preparing to import packages

The Afaria Service Account—the account used to install Afaria on the server—must have at least “Read” permissions on the SMS Server Distribution Point in order to import a package. If you have access to multiple Distribution Points within the same site, the Afaria Service Account must have “Read” permissions on each Distribution Point.



The Distribution Point must contain source files in order for the import process to work. For example, assume that you have access to multiple SMS server sites and that one of the sites created a package that has been made available to some of the SMS server sites, but not all. You may be able to view that package, but if it isn't available at the Distribution Point to which you have connected, package import will not take place.

Use the Software Distribution Properties dialog from the SMS Administrative Console to set and specify the drive path where the SMS packages are stored. If you do not specify the drive path, an error message will appear in the Messages Log on the Afaria Administrative Console.

In addition to the “Read” permissions noted above, if the Afaria Server and the SMS server belong to different domains, then you must add the Afaria Service Account to the SMS server's Local Users Group.

- **Automatically import channels.** You can select this option to automatically import software packages from the SMS server.
- **Import now.** You can select this option to manually import specific software packages from the SMS server.



Every SMS package you import into the server becomes a Software Manager channel for Windows Client types, regardless of the files included in the package.

Your imported packages will appear as Software Manager channels with the same name as the original SMS package. You can edit and deploy the channel in the same manner as other software channels that you create. Your Client users will not be able to distinguish between a channel created in Software Manager and a channel imported from an SMS server.

Channel settings

You can use the options in this area to pre-configure channel options for imported packages. You could also set these options for a Software Manager channel in Channel Administration.



When you build SMS software packages to import, do not select the SMS options to compress and/or encrypt the packages. Packages that are compressed/ encrypted in SMS can only be decompressed/ decrypted by an SMS Client, which may or may not be an Afaria Client. Instead, compress/encrypt imported SMS packages at the server.

- **Assign automatically.** When you select this option, the server automatically creates a Client group for each package imported from SMS and automatically assigns the imported package channel to the new Client group. The Client group should contain all Windows Clients that were in the collection to which the package was assigned in SMS.
- **Encrypt.** Automatically secures all information in transit so that unauthorized users cannot view it.
- **Authenticate.** Select this option to verify Clients' identities before making the channel's contents available to users.
- **Publish.** Automatically publish all imported packages.
- **AutoSubscribe.** All assigned Clients are auto-subscribed to the imported packages.
- **Assignments.** You can automatically assign, or map, all of the packages imported for a specific collection to one or more Windows user groups. When you click Assignments, the Assignments dialog box appears and lets you map the selected SMS Collection to the groups.



The assignments that you establish in this dialog box display on the Assignments property page in Channels Administration.

Check files options

You use these options to specify when to check a file on the Client. You can define these options for sets of channel files, as well as for a single file. The result of the selected Check file option will determine how Software Manager will execute the Send file options.

- **Always check file.** Set by default, this option checks any file every time the Client connects to the server. Use this option when files must be current with the server versions; it takes more time to execute, but it can replace files that are unintentionally deleted or modified at

the Client. Files that are missing or have changed at the Client are sent according to the Send file option you specify.

- **Only check file when package is updated.** When channel files at the server have been updated (either through changes you've made or through an automatic refresh in Channels Administration), Software Manager checks the corresponding files at the Client and then executes the Send file option you select.

Send file options

You use these options to specify when to send the file to the Client based on the result of the Check file options.

- **Send file when Server file is newer.** Sends files to the Client if the server copy is more recent than the Client copy (default). This option compares time and date stamps.
- **Send when Server file is different.** Set by default, this option sends the files to the Client if the server files are different. This option is useful when you want to send files to the Client that are older on the server. This option compares time and date stamps, or size.

Package settings

- **Synchronize SMS package settings.** This option instructs Software Manager to synchronize these settings in the packages:
 - Command Line
 - Package Comment

As long as you have selected this option, either of these changes in the SMS package is detected and reflected in the imported package during the scheduled refresh process or whenever you manually refresh the channel.

You can clear Synchronize SMS Package Settings if you determine that advanced options available in Software Manager bring you more benefits than staying synchronized with the SMS package settings. If most of your SMS packages remain unchanged after their creation, synchronization might be unimportant to you. In that case, you can turn this option off and use the Software Manager Channel Editor to add criteria checking, delivery and installation time frames, share mapping and other Software Manager features.

If you select synchronized settings you can still turn synchronization off when you open the Software Manager Channel Editor to make and save a change. You'll receive a message box notifying you that you are about to "unlink" the package.

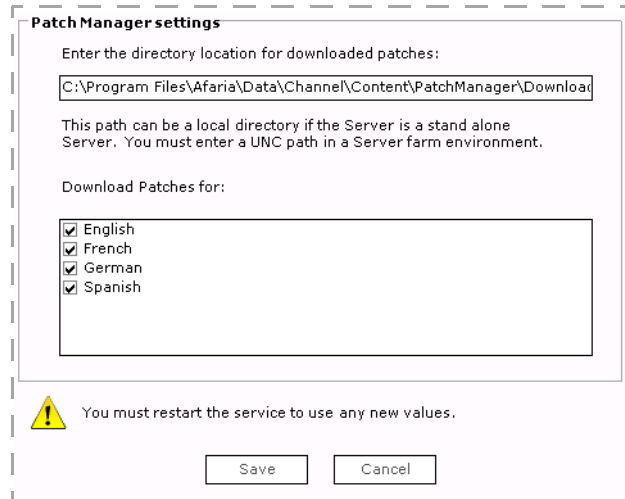
Once synchronization is turned off, you cannot turn it back on. However, unlinking the package does not affect the integrity or delivery of the imported package.

- **Start installation automatically on the Client.** Initiates installation of the package during the Client's connection to the server.

- **Difference all files.** Set by default, this option detects, extracts, and sends only byte-level file differences, reducing the time required to update files and software.
- **Local install.** Set by default, this option sends the package to a staging area (temporary area) on the Client. The installation can then run offline, without connecting to the server.

Patch Manager

You must establish a valid download location for all Microsoft patches you download to deploy over Patch Manager channels.



The screenshot shows a dialog box titled "Patch Manager settings". It contains a text input field with the path "C:\Program Files\Afaria\Data\Channel\Content\PatchManager\Download". Below the input field is a note: "This path can be a local directory if the Server is a stand alone Server. You must enter a UNC path in a Server farm environment." Underneath is a section "Download Patches for:" with a list of languages: English, French, German, and Spanish, each with a checked checkbox. At the bottom, there is a warning icon and the text "You must restart the service to use any new values." and two buttons: "Save" and "Cancel".

You can change the default location to one that is appropriate for your environment.



- The download path must be a UNC path with domain/LDAP level credentials. You may use a local path only in the case of a standalone server.
- The Afaria service account that you established during the Afaria installation process must have access to the download path.
- Refrain from using mapped drives in your download path.
- A single, shared patch download location is recommended for server farms. [“Downloading patches for server farms” on page 218.](#)

Patch Manager requires additional steps before you can start using the Configuration's Patch console, Patch Manager channels, or the Client patches view. See [“Patch console” on page 212](#) for required action. See *Afaria Reference Manual | Components, Patch Manager*, for additional information.

Server schedules



From the Server schedules area, you can define a schedule for tasks you perform on a regular basis, such as updating channel content or distributing software, so that these tasks run automatically at regular intervals. The **Server schedules** folder contains several predefined schedules you can edit to meet your needs.

See also [“Edit existing schedules” on page 187](#).

Server Configuration > Server Schedules

Server schedules	Client Group Auto Refresh
Server schedules	Name Client Group Auto Refresh
AV/Firewall Version Tracking	Description Updates members of dynamic Client groups
Cleanup Deleted Channels	Summary At 12:00:00 AM every day
Client Group Auto Refresh	Edit
Compression Refresh	Run now
Differencing Refresh	
License Compliance Refresh	
Log Cleanup	
Patch List Synchronization	

All schedule settings are saved in the following location:

<ServerInstallDir>\Data\Channel\Listings\

The predefined schedules on your server include:

- AV/Firewall Version Tracking – Populates the database with AV/Firewall client version tracking information, as collected from the connecting clients since the last time the schedule ran. This data is reflected in data views and reports.
- Cleanup Deleted Channels – Permanently removes all channels that were deleted from the server more than 60 minutes prior to the schedule's run time.
- Client Group Auto Refresh – Automatically updates dynamic Client groups.
- Compression Refresh – Updates all data in the compression cache.
- Differencing Refresh – Updates all data in the differencing cache.
- License Compliance Refresh – Updates license compliance summary information.
- Log Cleanup – Permanently removes selected records from the log database.
- Patch List Synchronization – Updates the Microsoft patch list that displays in the Patch console and downloads any patches that you select on the Patch console.

In a server farm, the schedule runs for only one server at a time. Therefore, configuring all servers in a farm with the same schedule results in only one server downloading the patches. See [“Downloading patches for server farms” on page 218](#).

- SMS Refresh – Updates all SMS imported software channels.
- Update AV/Firewall Definitions – Contacts the AV/Firewall update server and retrieves any new virus definition files and client files.
- Update Channel Contents – Updates the contents of all channels on the server.

To run a predefined server schedule at any time, you can select the schedule in the left pane and click **Run now** in the right pane.

Edit existing schedules

You can edit server schedules by selecting a schedule in the left pane and clicking the Edit link in the right pane. The Schedule Editor appears and displays the Schedules page.

Server Configuration > Server Schedules > Edit > Schedule

The Schedule Editor's Schedule page contains the following fields:

- Name – The schedule name.
- Description – A brief explanation of the schedule's purpose.
- Schedule type – Displays the type of schedule: Daily, Weekly, Monthly, Once, or Online. You can select a new schedule type from the drop-down list.
- Start time – Displays the current start time for this schedule. You can change the start time and also run the schedule at startup if the schedule is missed.
- Schedule Task area – Displays the options for the type of schedule selected:
 - Daily or Weekly – Displays the days of the week.
 - Monthly – Displays the months of the year.
 - Once – Does not display any information.
 - Online – Displays the Internet access parameters.

The screenshot shows the 'Advanced' tab of the 'Schedule' editor. The schedule name is 'Cleanup Deleted Channels' and its description is 'System schedule to remove deleted channels'. The schedule type is set to 'Daily' in a dropdown menu. The start time is '12:00:00 AM'. There is a checkbox for 'Run at startup if schedule was missed' which is currently unchecked. Below this, the 'Schedule task daily' section is visible, showing 'Every 1 day(s)'. Underneath, a box titled 'On the following day(s):' contains seven checked checkboxes for the days of the week: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.

Server Configuration > Server Schedules > Edit > Advanced

Depending on the schedule type, the Schedule Editor's Advanced page contains the following fields:



When you edit "Once" schedules, no fields appear on this page. When you edit "Online" schedules, the **Specify a date range** field appears.

- Specify a date range – Displays the date range for this schedule. You can change the date range by selecting a new date from the **Begin** and **End** spin boxes.
- Repeat – Displays the parameters for repeating the scheduled task. You can edit any of the fields in this area.
- Retry – Displays the number of times Afaria should attempt to retry running the scheduled task. The **Retry interval** specifies the time period. You can edit either of these fields.
- Randomize start time by – Displays the parameters for randomizing the start time for the scheduled task. You can change the time by selecting values from the spin boxes.

Schedule **Advanced**

You can specify a date range. If a date range is specified, this task will only run during this range. If no range is specified, the schedule is always active.

Specify a date range

Begin End

Schedules can be set up to run at a specific time or on a recurring basis.

Repeat

Every

Until this time

For hour(s) minute(s)

Retry time(s) Retry interval minute(s)

Randomize start time by hour(s) minute(s)

Client types

Use the Client types area to add or customize supported Client types on your server. Client types are not the same as Client groups. Client groups are groups to which you can assign channels; they are device-based and depend on data queries you create in Data views, Clients. With Client types, you use Afaria's supported Client types to create "custom" Client types for which you can create Client executables or Afaria channels. For example, you may have some users running the Afaria Client on Windows XP laptops. You can create a Client type called "Windows XP laptops" and specify parameters, such as the operating system, the operating system version, and any service packs that have been applied. Then, when you create channels in **Administration > Channel Administration**, you can create the channel specifically for the Windows XP laptop Client type.

Server Configuration > Client Types

Client types	
[-] All Client Types	
[-] All Windows Clients	
[-] Windows Clients	
[-] BlackBerry Clients	
[-] All BlackBerry devices	
[-] Java Clients	
[-] All Java Clients	
[-] OMA-DM Clients	
[-] All OMA-DM Clients	
[-] Palm Clients	
[-] Palm OS Version 5.x	
[-] Symbian Clients	
[-] All Series 60 Clients	
[-] Windows Mobile Professional Clients	
[-] All Windows Mobile Professional Clients	
[-] Pocket PC/Windows CE with StrongArm processor	
[-] Windows CE with ARM Thumb processor	
[-] Windows Mobile Standard Clients	
[-] All Windows Mobile Standard Clients	

All Client Types	
Client details	Detail value
Description	All Client Types
Operating System	
Operating System Version	
Processor	
Service Pack	
Operating System Type	

The left pane contains all of the supported Client types. The contents of the right pane depends on the item selected in the left pane. You may see the following values: description, operating system, operating system version, processor, service pack, and operating system type.

Add a new Client type

Supported Client types – Afaria Clients

Server Configuration > Client Types > Client type > New based on



You can add a new Client type by selecting the Client type on which you want to base the new Client type, such as “All Java Clients,” and clicking **New** on the toolbar. Alternately, right-click a Client type in the left pane and select **New based on**.

You must enter a value for at least one of the available data items.

- Description – A unique identifier for this Client type.
- Operating system – Operating system.
- Operating system version – The version number of the operating system, such as “5.0”.
- Processor – The processor, such as “StrongArm” for the Windows Mobile Professional Client type. The acceptable values for this field appear on the Client types page for relevant Client types.
- Service pack – Service pack number, such as “6a”.
- Operating system type – An operating system type.

Create new based on Java Client

To create a new Client type definition, you must specify a value for at least one of the following six parameters. The value you specify is checked against the value returned by the device. The values are checked character by character from left to right.

Description
Java Client

Operating system

Operating system version

Processor

Service pack

Operating system type
<none>

OK Cancel

Setting parameters for Windows Client types

When you create a Windows Client type, the service pack information is equal to or greater than (= or >) what is specified. For example, if you create a Client type with the following parameters:

Operating System Version: 2000

Service Pack: 4

OS Type: Windows 2000 Clients

any associated channel is delivered to a Windows 2000 Client with Service Pack 4, but not to a Windows 2003 Client.

Setting parameters for Windows Mobile Professional Client type

When you create a Windows Mobile Professional Client type, the Device Type and Processors are enabled. For example, if you enter StrongARM as the Processor, any associated channel is delivered to a StrongARM device, but not to any devices running other processor types.

Edit Client type properties

Server Configuration > Client Types > Client type > Properties



Select a type in the left pane and click **Properties** on the toolbar, or right-click the Client type and select **Properties**.



If you select a predefined Client type and click Properties, the Examine Client type definition dialog box appears. This dialog box is similar to Edit Client type definition, except the fields are *read-only*.

You cannot edit any of the existing Client type categories in the Edit Client type definition dialog box; to “edit” a predefined Client type, you must make a new Client type based on the existing one with exactly the same properties, then specify the new parameters for that Client type.

Edit Client type definition

To create a new Client type definition, you must specify a value for at least one of the following six parameters. The value you specify is checked against the value returned by the device. The values are checked character by character from left to right.

Description
Java Client

Operating system

Operating system version

Processor

Service pack

Operating system type
<none>

OK Cancel

Alert definitions

From the Alert definitions area, you can define events that trigger alerts on your server. These alerts, which appear on the Home, Alerts window, notify you when some incident arises on your server or its components, so you can acknowledge and resolve it quickly. For more information about viewing and resolving raised alerts on your Afaria Server, see [“Alerts” on page 72](#).

Click **Server Configuration** on the global navigation bar and select **Alert definitions** from the drop-down menu to access Alert definitions. The Alert definitions window appears.

Server Configuration > Alert Definitions

Alerts					
Raised alert	Description	Time opened	Time acknowledged	State	Contact
<input type="checkbox"/>	Maximum Number of A Specific...	A specific registered aler...	12/2/2008 2:53:58...		Unacknowl...
<input checked="" type="checkbox"/>	A Custom Alert	User defined custom alert...	12/2/2008 2:57:08...	12/2/2008 3:36:16...	Acknowled...
<input checked="" type="checkbox"/>	Alerts Console - A specific re...	A specific registered alert...	12/2/2008 2:53:58...	12/2/2008 3:36:21...	Acknowled...
<input checked="" type="checkbox"/>	Backup Manager - Final disk ...	The final used disk space ...	12/2/2008 2:56:08...	12/2/2008 3:36:26...	Acknowled...
<input checked="" type="checkbox"/>	Backup Manager - Initial disk ...	The initial used disk spac...	12/2/2008 2:57:53...	12/2/2008 3:36:28...	Acknowled...
<input checked="" type="checkbox"/>	Backup Manager - Middle disk...	The middle used disk spac...	12/2/2008 2:57:53...	12/2/2008 3:36:31...	Acknowled...
<input type="checkbox"/>	Backup Manager - Pending re...	A backup cannot proceed...	12/2/2008 2:57:53...		Unacknowl...
<input type="checkbox"/>	Client - Client diff cache full	The Client File Differencin...	12/2/2008 2:57:44...		Unacknowl...
<input type="checkbox"/>	Client - Client diff cache high	The Client File Differencin...	12/2/2008 2:57:43...		Unacknowl...
<input type="checkbox"/>	Client - Client diff cache low	The Client File Differencin...	12/2/2008 2:57:42...		Unacknowl...
<input type="checkbox"/>	Client - Client diff cache medi...	The Client File Differencin...	12/2/2008 2:57:43...		Unacknowl...
<input type="checkbox"/>	Configuration Manager - Cont...	The user_exports the dat...	12/2/2008 2:57:54...		Unacknowl...

You will see three property page tabs in the Alert definitions area:



You can click the column headings on each page to sort the information in each column.

Defined alerts. The Defined alerts property page displays the following information:

- *Alert name.* The name you assigned to the alert.
- *Description.* The description you assigned to the alert.
- *Contact.* The name of the contact, if any, you associated with the alert.
- *Threshold.* The number of times an event or set of events must occur during a certain time period in order to raise an alert.
- *Threshold interval.* The window of time during which the threshold number of events must occur in order to trigger an alert.
- *State.* The state of the alert, either Enabled or Disabled.

The alerts listed on this page are only the alerts you have defined on your system. All raised alerts display on the Alerts page in the Home area of your server. For more information, see [“Alerts” on page 72](#).

Defined events. The Defined Events property page displays information about system-defined and user-defined events on your system: the Event name, Description, and the Component. In this context, *component* is a general category for grouping events based on a functional area of the product. If the event is user-defined, this information displays in the Component column.

Defined contacts. The Defined contacts property page displays each contact's Name and Pager and/or E-mail address.

Configure alert options

Before you define any alerts, you should determine how you will respond to alerts raised on your server. Consider these questions:

- What events will trigger an alert?
- Will you use system-defined events to trigger alerts, or do you need to define your own?
- Who will be responsible for handling raised alerts, and how will they be contacted?
- Will you have your system forward an SNMP trap or run an executable file in response to certain alerts?


Once you have considered these and other questions, you should:

- “[Define custom events](#)” you want to trigger alerts.
- “[Create a contact list](#)” of people you want the system to contact when an alert is raised.
- “[Define alert response options](#)”, such as your mail server and your SNMP IP address.

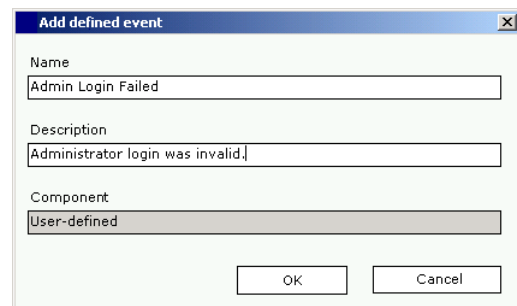
Once you have completed these tasks, you will be ready to define your alerts.

Define custom events

The server contains a number of system-defined events that you can assign to alerts, but you can define events that will work alone or together with other system-defined events to trigger an alert on your system. Any event you define on your server will appear as “User-defined.”

To define an event, you click  **New, Event** on the toolbar, and the Add defined event dialog box appears. You can enter a name and description for the event. The name must be unique; you cannot have two events with the same name, even if the descriptions are different. The Component field reads “User-Defined” and is uneditable. This helps you differentiate user-defined events from system-defined events.

When you click **OK** to add the event, it appears in the list on the Defined events property page.



Add defined event	
Name	Admin Login Failed
Description	Administrator login was invalid.
Component	User-defined
OK Cancel	

Edit an event



You cannot edit or delete system-defined events.

You can edit an event by selecting it on the Defined events page and clicking **Edit** on the toolbar, or double-clicking the event in the list. The Edit event dialog box appears. You can change the necessary information and click **OK** to return to the Defined events page. The updated event information appears in the list.

If you want to delete an event, select it in the list on the Defined events page and click **Delete**. The event is permanently removed from the list.

Edit event

Name
Admin Login Failed

Description
Administrator Login was invalid

Component
User-defined

OK Cancel

Create a contact list

The Defined contacts page lists all of the contacts you have defined on your server. When you first install and run your server, you will notice that this page is blank. To add a new contact, you click **New, Contact** on the toolbar. The Add contact dialog box appears. Use this to add contacts the system will alert when specific alerts are raised. You designate these contacts when you define your alerts.

You must enter the following information for the contact: a unique **Name**, a numeric **Pager address**, such as 555-1234@mypager.net, and/or the **E-mail** address for the contact, such as johndoe@mycompany.com.

When you click **OK**, if you have not defined your mail server, the Contacts message box appears. For more information on defining your mail server, "[Define alert response options](#)" on page 196. You can click **Yes** on the Contacts message box to continue. A message box appears telling you the contact has been added to the Defined contacts list.

Add contact

Name
John Smith

Pager address
555.1234@myservice.net

E-mail
js.smith@mycompany.net

OK Cancel

Message


Pager or e-mail will not work until the mail server has been defined.
You can define the mail server in the Alert response options dialog box.


OK



Even if you add a contact, that contact is not valid until you have defined a host name for the mail server.

Edit the contact list

You can edit a contact's information by selecting it on the Defined contact page and clicking  **Edit** on the toolbar, or double-clicking the contact in the list. The Edit contact dialog box appears. You can change the necessary information and click **OK** to return to the Defined contacts page. The updated contact information appears in the list.


If you want to delete a contact, select it in the list on the Defined contacts page and click  **Delete**. The contact is permanently removed from the list.

Define alert response options

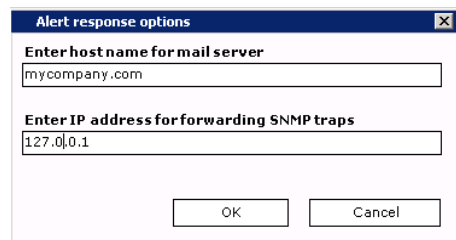
When you define an alert, you determine whether you want your server to contact a person via e-mail or page or forward an SNMP trap. You must designate the mail server where your contacts reside or the IP address where you can forward SNMP traps.



If you are planning to use SNMP in a server farm scenario, all servers in the farm must have SNMP installed and configured the same way. Each server in a farm scenario must also specify the same mail server.

To configure alert response options, you click  **Alert response options** on the toolbar. The Alert response options dialog box appears.

You can enter a host name for the mail server, such as mycompany.com, or enter an IP Address, for forwarding SNMP traps.



The dialog box titled "Alert response options" contains two text input fields. The first field is labeled "Enter host name for mail server" and contains the text "mycompany.com". The second field is labeled "Enter IP address for forwarding SNMP traps" and contains the text "127.0.0.1". At the bottom of the dialog box are two buttons: "OK" and "Cancel".




If SNMP is not installed on the server, the Enter IP Address for forwarding SNMP trap area is disabled.

Define an alert

When you define an alert, you determine:

- Which events raise an alert
- How often an event or combination of events must occur before an alert is raised
- Who will be contacted or what action will be taken once an alert is raised
- How often an alert response will repeat until someone acknowledges it.

You define an alert by selecting  **New, Alert** on the toolbar. The Alert definition wizard appears. When you step through this wizard, you complete these tasks:

[“Set alert properties” on page 198](#). In the Alert properties dialog box of the wizard, you set general properties, such as the alert name, description, and priority. You also enable or disable alerts from here.

[“Assign events to an alert” on page 198](#). In the Assigned events dialog box, you select the events you want to trigger the alert. You can also remove events from an alert.

[“Set the alert threshold” on page 199](#). In the Alerts threshold dialog box, you determine how many times an event or a combination of events must occur during a specified time period before an alert is raised on your system.

[“Choose an alert response” on page 200](#). In the Alert response dialog box, you specify how your Afaria system will respond to an alert: by contacting a person, sending an SNMP trap, running an executable file, or any combination of these options.

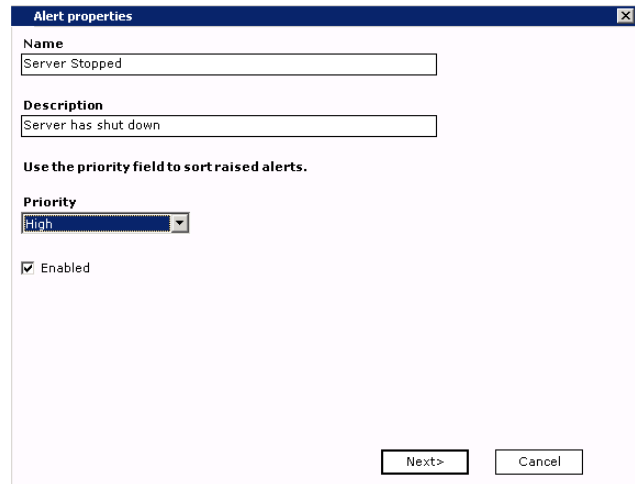
[“Repeat alert responses” on page 201](#). In the Alert response repeat interval dialog box, you determine how many times an alert response will repeat until someone acknowledges the alert.

Once you have completed these tasks, the alert appears in the list of defined alerts on the Defined alerts tab. You can edit any of the alerts in this list as long as it is not currently raised on the system.

Set alert properties

You use the Alert properties dialog box or property page to define or edit an alert's general properties, such as **Name**, **Description**, and **Priority**. You also enable and disable alerts from this dialog box. Alerts will not be raised on your system until you enable them.

You click **Next** to continue defining your alert. The Assigned events dialog box appears.



The 'Alert properties' dialog box contains the following fields and controls:

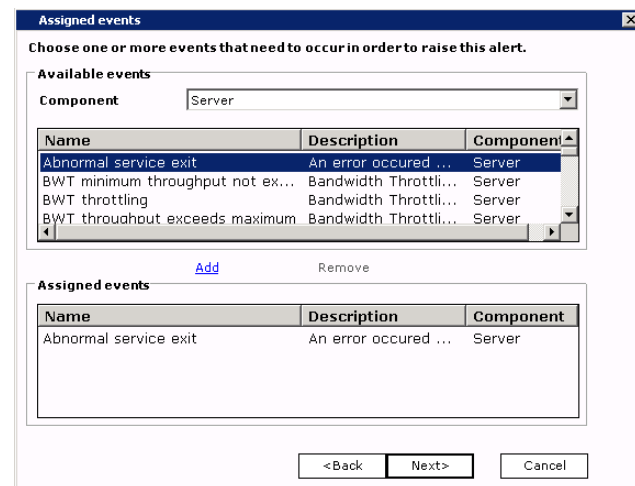
- Name:** Text box containing 'Server Stopped'.
- Description:** Text box containing 'Server has shut down'.
- Priority:** A dropdown menu currently set to 'High'. Above it is the instruction: 'Use the priority field to sort raised alerts.'
- Enabled:** A checked checkbox.
- Buttons:** 'Next>' and 'Cancel' buttons at the bottom right.

Assign events to an alert

Use the Assigned events dialog box or property page to assign events to or remove events from an alert. You can specify any combination of system-defined and/or user-defined events to trigger an alert.

In the **Components** drop-down list box, *All Components* shows as the default.

- If you want to select events for a specific component, you must select the component from the list. The system-defined events for the component you selected appear in the Available Events list box.
- If you want to select an event you defined, you must select *User-defined* from the Components drop-down list.



The 'Assigned events' dialog box contains the following elements:

- Title:** 'Assigned events'.
- Instruction:** 'Choose one or more events that need to occur in order to raise this alert.'
- Component:** A dropdown menu set to 'Server'.
- Available events:** A table with columns 'Name', 'Description', and 'Component'.

Name	Description	Component
Abnormal service exit	An error occurred ...	Server
BWT minimum throughput not ex...	Bandwidth Throttli...	Server
BWT throttling	Bandwidth Throttli...	Server
BWT throughout exceeds maximum	Bandwidth Throttli...	Server
- Assigned events:** A table with columns 'Name', 'Description', and 'Component'.

Name	Description	Component
Abnormal service exit	An error occurred ...	Server
- Buttons:** '<Back', 'Next>', and 'Cancel' buttons at the bottom.

You add an event by selecting it from the list box and clicking **Add**. The event appears in the Assigned events list box. You can remove an event from the Assigned events list by selecting it in the Assigned events list box and clicking **Remove**.

You click **Next** to continue defining your alert. The Alerts threshold dialog box appears.

Set the alert threshold

You use the Alerts threshold dialog box to specify the number of times an event or set of events must occur during a certain time period in order to raise an alert.

In the **Number of event occurrences** spin box, you can select the number of times the event(s) must occur in order to raise an alert. For example, you might decide an event or set of events must occur five times in order to raise an alert.



If you have assigned more than one event to an alert and you specify an event must occur five times in order to raise an alert, *any combination* of these events occurring five times will raise the alert.

Alerts threshold

Select the number of assigned events that must occur during a specified time period in order to raise this alert.

Number of event occurrences 1

Time period

Unlimited

Hour(s) 1

Day(s) 1

<Back Next> Cancel

In the **Time period** area, you can select one of the following time frames in which the events should occur:

- If you want an alert to be raised as long as the events occur the specified number of times, you should select **Unlimited**. If you selected five as the number of event occurrences, then the event must occur five times before the alert is raised, whether it occurs over a period of ten hours or ten days.
- If you want the number of events to occur within a specified time period, then select **Hours** or **Days** and a number from the spin box. For example, you might specify an event must occur five times over the next 30 days in order to raise the alert.

You click **Next** to continue defining the alert. The Alert response dialog box appears.

Choose an alert response

You use the Alert response dialog box to determine how you want the server to respond when an alert is raised:

- Notify a contact
- Send an SNMP trap
- Run an executable file

To assign a contact to the alert, you select the **Contact** check box, and then select a name from the drop-down list box. If you have not added any contacts, this area is disabled. For more information on defining contacts for alerts, [“Create a contact list” on page 195](#).



If you plan to run an executable file in a server farm scenario, all computers in the farm must configure the location of the executables in the same manner in order for the executable to run when the alert is raised.

Alert response

Select actions server should take when the alert is raised.

Contact
John Smith

Page E-mail

Message text for page/e-mail
Please contact us as soon as possible

Send SNMP trap

Run executable Browse...

<Back Next> Cancel

If you have defined contacts but have not defined a mail host, a message box appears alerting you that you must define a mail host. You can click **OK** to continue defining the alert, but you must define the mail host or the alert response will fail. For more information on setting up a mail host, [“Define alert response options” on page 196](#).



You can select either or both the **Page** and **E-mail** check box(es) to determine how the system should notify the contact you specified about the alert.

In the **Message to use for page/E-mail area**, you can enter a message (up to 255 characters) regarding how the contact should handle the alert. For example, do you want the contact to check the server, or notify a supervisor?

You select the **Send SNMP trap** check box to enable an SNMP trap to be raised on the server. If SNMP does not exist on the server, this option is disabled. For information on forwarding an SNMP trap to another computer besides the server, [“Define alert response options” on page 196](#).

You can also have the system run an executable file or batch file by selecting the **Run executable** check box, then entering the file path and name, or clicking **Browse** to locate the *.exe or *.bat file you want to run.

You click **Next** to continue defining the alert. The Alert response repeat interval dialog box appears.

Repeat alert responses

You use the Alert response repeat interval dialog box to specify how often you want the system to repeat the specified response until the alert is acknowledged. For example, if you specified that you want to page Mary Smith when an alert is raised, you may select that you want the system to page her every day until she acknowledges the alert.

In the Interval area, you can select one of the following options for how often you want the alert response to repeat.

- **Do not repeat response.** This option causes the alert response occur only once when the alert is raised.
- **Hour(s).** This option causes the alert response to repeat every n hours. You can select the exact number from the spin box.
- **Day(s).** This option causes the alert response to repeat every n days. You can select the exact number from the spin box.

To determine the maximum number of times you want the response to repeat, you can select a number from the **Repeat** spin box. For example, if you chose to have Mary Smith paged every day, you would select five (5) to have her paged every day for five days until she acknowledges the alert.

You click **Finish** to add the alert to your system or click **Back** to change any values for the alert.

Alert response repeat interval

Select how often the Alert Response will be repeated until the alert is acknowledged.

Interval

Do not repeat response

Hour(s) [spin box]

Day(s) [spin box]

Repeat [spin box]

<Back Finish Cancel


Edit an alert

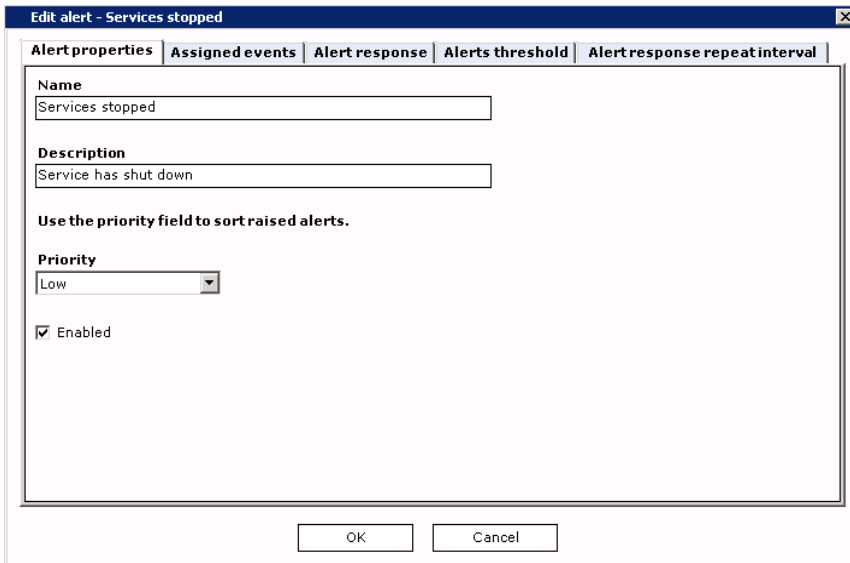
You can edit any defined alert on your system as long as there are no alerts of that type currently raised on your system.

When you edit an alert, changing any of the following attributes significantly alters the alert:

- Adding or removing events
- Changing the threshold time
- Changing the threshold interval

When you edit events or threshold counts associated with an alert, any current raised events that were associated with the original alert are no longer associated with the pending alert.

To edit an alert, you can select it and then click  **Edit** on the toolbar, or you can double-click the alert on the Defined alerts page. The Edit alert dialog box appears. The name of the alert you are editing appears in the title bar.




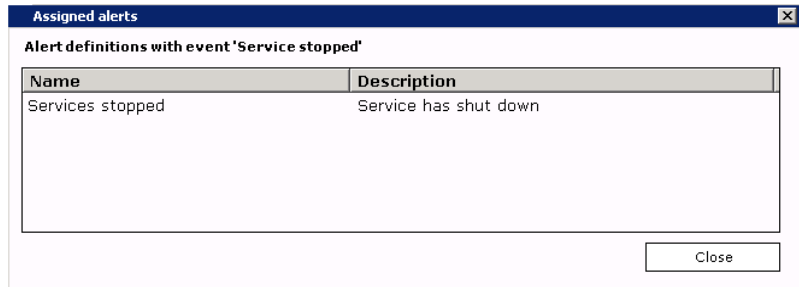
The screenshot shows a dialog box titled "Edit alert - Services stopped". It has five tabs: "Alert properties", "Assigned events", "Alert response", "Alerts threshold", and "Alert response repeat interval". The "Alert properties" tab is selected. Inside the dialog, there is a "Name" field containing "Services stopped", a "Description" field containing "Service has shut down", a "Priority" dropdown menu set to "Low", and a checked "Enabled" checkbox. At the bottom of the dialog are "OK" and "Cancel" buttons.

You will see five property pages. You can click the following property pages to complete the corresponding tasks. Notice that these pages correspond exactly to each of the dialogs in the Alert definition wizard.

- **Alert properties.** [“Set alert properties” on page 198.](#)
- **Assigned events.** [“Assign events to an alert” on page 198.](#)
- **Alerts threshold.** [“Set the alert threshold” on page 199.](#)
- **Alert response.** [“Choose an alert response” on page 200.](#)
- **Alert response repeat interval.** [“Repeat alert responses” on page 201.](#)

View event alert assignments

You can view the alerts associated with both system and user-defined events. To view alert assignments, you select an event on the Defined events page and click  **View assigned alert**. The Assigned alerts window appears and lists the name and description of the alert to which the event is assigned. You can click **Close** to return to the Defined events page.

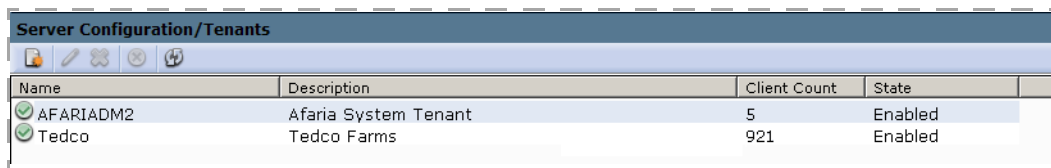


Tenants

Support – Multitenancy only

Use the Tenants page to maintain tenant records. A *tenant* is an entity that you associate 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. See [“Using Tenants and Multitenancy” on page 23](#) for general multitenancy information and workflow.

Server Configuration > Tenants



Name	Description	Client Count	State
AFARIADM2	Afaria System Tenant	5	Enabled
Tedco	Tedco Farms	921	Enabled

The Tenant page displays the following data elements:

- Name and Description – user defined values
- Client count – the number of clients connected and assigned to the tenant
- Status – the state of the tenant:
 - Enabled – associated clients can connect and have sessions and Afaria Administrator users can operate and support the tenant.
 - Disabled – associated clients can connect but are denied running sessions. However, the existing data remains accessible to Afaria Administrator users.

You can change a tenant’s status at any time.

Adding a Tenant

Add a tenant to establish an entity for associating clients, assets, and related data.

- 1 On the Tenant page, right-click on any row and select **New**.
- 2 Enter a name and description.
- 3 Select or clear the **Enabled** check box to define the tenant state.

See [“Defining a Role’s Tenant List” on page 45](#) to define which tenants a roles’ users can access.

Disabling a Tenant

Disable a tenant when you want to prevent clients from running sessions for a tenant but want to preserve all the tenant's existing data. You can disable a tenant on a temporary or permanent basis. You cannot disable the system tenant.

- 1 On the Tenant page, right-click on the tenant and select **Disable**.

The system raises an event anytime a client attempts to run a session for a disabled tenant. See [“Define an alert” on page 197](#) if you want to the system to open an alert if such an event occurs.

Deleting a Tenant

Delete a tenant when you want to permanently remove a tenant from your system. You cannot delete the system tenant. The scope of the tenant delete action includes deleting clients and client groups.

If you plan to delete a tenant, you are advised to first delete the tenant-based items that are outside the scope of the tenant delete action:

- Channels
- Client backups
- Client patches
- License compliance
- Logs
- Monitors
- Package tracking
- Policies
- Profiles

This tenant data is subject to becoming orphaned during a tenant delete action.

- 1 On the Tenant page, right-click on the tenant and select **Delete**. The confirmation dialog box indicates the scope of the related delete actions.
- 2 Click **OK** to continue.

Afaria Administrator users that have their browser open to the Afaria Administrator interface when the delete action executes must restart their browser to reflect the update.

License compliance

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

License Manager supports all versions of Client operating systems that are supported by Inventory Manager; however, all Client types will not have exactly the same level of supported data. For instance, version isn't tracked on Symbian and BlackBerry Clients; and software size isn't tracked on Windows or Windows Mobile Professional Clients.



You must have *Create* permission in Access policies in order to add software licenses to the database.

Create license definitions


The License compliance page appears empty until you define software licenses in your database. Once you have defined these software licenses, the page displays data for Client category, Manufacturer, Application, Size, Version, # (number) Purchased, Effective and Expiration dates, and any Notes you may add. Initially, licenses are sorted by Client category, Manufacturer, then Application.



You can change the order in which the data appears by grabbing a column header and dragging it to a new location; you can also change a column's sort order by clicking its heading.

Server Configuration > License Compliance

License compliance						
Client category	Manufacturer	Application	Size	Version	# Purchased	Effective date

Click  **New** on the button bar to display the submenu, then select the Client category for which you want to define a software license. The License data dialog box appears.

You can also right-click the page to display the **New** shortcut menu.

License data

Client category Palm

Application definition
Enter information that uniquely identifies the application.

Name

Version (Optional) Version may contain a single wildcard character (*). For example 2.3*

Size (in bytes) (Optional)

[Select from inventory data...](#)

License information
Enter information that details licenses purchased.

Effective date 12/ 4/2008

Expiration date 12/ 4/2008

Number purchased 1

Description
Enter further descriptive information if required.

Manufacturer

Notes

OK Cancel



License Manager is mapped to Inventory Manager scans via the name, size and version information (if specified) in the license definition. These three items must match exactly the records in the inventory database in order to track license data.



Running an inventory scan does *not* update license compliance summary data nor fire events. Only refreshing the License Compliance Refresh Server schedule performs these actions. You can run the system schedule that refreshes the license compliance tables from the License compliance page just by clicking the **Recompute** button on the button bar. For details on working with server schedules, see “Server schedules” on page 186.

Ensure that *Client category* displays the type of Client for which you want to enter license data, then enter up to 255 alphanumeric characters to represent the **Name** of the application.



The Name must exactly match the records in the inventory database. You may find it helpful to select from existing inventory data in the Inventory data selection dialog box.



The Name field is the only required field on this dialog box.

If the Client category allows you to track the **Version** of the application, you may enter up to 255 alphanumeric characters, including a single wildcard symbol in the *last* position, in the field provided.



If Version is not defined, an asterisk (*) wildcard character will display when you re-access the License data dialog box.

If Version includes a wildcard character, that character is visible in all places in which Version displays. If the Version's leading characters exist in another definition such that the same installation data would be reported for multiple license definitions, a warning message displays. Examples of *overlapping* license information may be, 2.1.* is entered when 2.1.5033.23 exists; 4.5.231 is entered and 4.5* exists; or ApplicationName 7.5* is entered and ApplicationName * exists.

If the Client category allows you to track the **Size** of the application (Palm, Symbian, and BlackBerry), you may enter a numeric value up to 2147483647 (without commas) in the field provided.

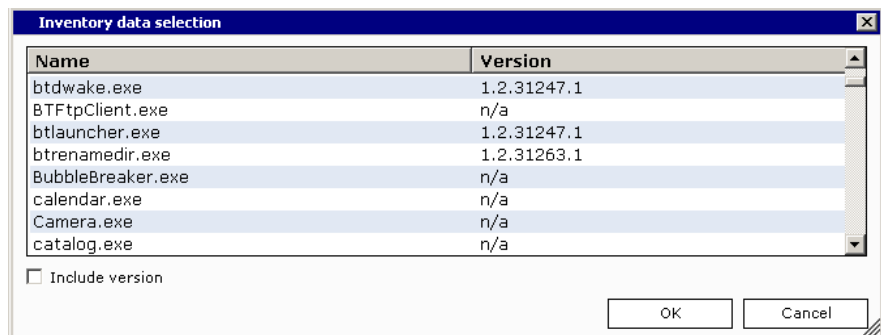
To choose from a list of software applications that already exist in your database, click the **Select from inventory data** link. The Inventory data selection dialog box appears.



Depending upon the selected Client category, the Inventory data selection dialog box will display the Include version and Include size check boxes, the Include version check box, the Include size check box, or neither check box.

Select the row representing the application for which you want to create a license definition and then click **OK** to quickly fill in the Name field in the License data dialog box.

If available, select the **Include version/Include size** check boxes to include Version/Size field data in the License data dialog box.



To enter an **Effective date** (the date on which the license becomes valid), select the check box then click the drop-down arrow to choose the date from the calendar. You can also enter the date in the field provided.

To enter an **Expiration date**, repeat the step above.



If the Effective date check box is selected, then the date entered must not be later than the Expiration date, if one is defined; however, Effective and Expiration dates can be the same.

Enter the **Number purchased** in the field provided. The number cannot exceed one million and cannot contain commas.

To further describe the software, enter up to 255 alphanumeric characters to represent the name of the **Manufacturer**.

Enter any **Notes** you want to track. Notes may contain up to 4000 alphanumeric characters.

Click **OK** to save the information to the database. The license definition appears on the License compliance page.

Server Configuration > License Compliance

License compliance					
Client category	Manufacturer	Application	Size	Version	#
Windows	Ghost Mfg	Ghost		*	1
Windows	iAnywhere Solutions, Inc	Afaria		*	15
Windows	Microsoft	Cinematronics 3D Pinball		5.1	15
Windows	Microsoft	Internet Explorer		*	20
Windows	Network Associates	Network Associates McAfee Alert Manager		*	20
Windows	Network Associates	Network Associates NetShield and VirusScan for NT and 2000		*	20



As license data becomes available it displays on the License compliance page.



Any successful additions, changes, and deletions to license definition data generate messages that display in Data views, License compliance. For details on working with Data views to track compliance and usage data, [“Tracking Software Compliance and Usage Data” on page 482](#).

Work with existing license definitions

If you’ve been granted *Create* or *Modify* permissions in Access policies, then you can work with existing license definitions.

Copy

Create permission allows you to copy—clone—the contents of an existing license definition to create a new definition.

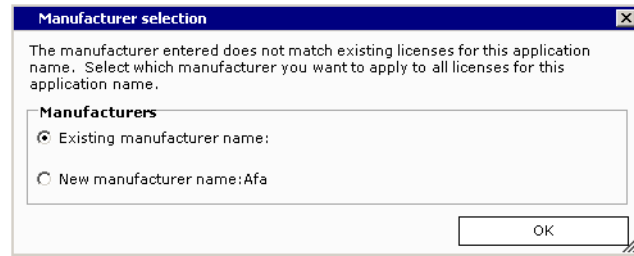
To create a license definition by copying an existing definition, select the row containing the definition you want to clone, then click **Copy** on the button bar. The License definition dialog box appears displaying the details of the selected row.

You can also right-click the row and choose **Copy** on the shortcut menu.

Modify the information to *create* the new definition, then click **OK** to save it to the database.



When you enter the name of the Manufacturer it must be identical to that of previous records or you will be prompted to choose the correct name in the Manufacturer selection dialog box. All records will reflect the name you select. Click **OK** to save your selection.



Edit

Modify permission allows you to edit an existing license definition.

To edit an existing license definition, select the row containing the definition you want to modify, then click **Edit** on the button bar. The License definition dialog box appears displaying the details of the selected row.

You can also double-click the row or right-click the row and choose **Edit** on the shortcut menu.

Make the changes necessary, then click **OK** to save the changes to the database.

Changes you make to the name of the Manufacturer of the same application will be reflected across all like records.

Delete

Modify permission allows you to delete an existing license definition.

To delete an existing license definition, select the row containing the definition you want to delete, then click **Delete** on the button bar. Afaria prompts you to confirm the deletion.

You can also right-click the row and choose **Delete** on the shortcut menu.

Click **Yes**.

Set compliance event thresholds

License Manager provides five, predefined events that fire when specific criteria is met. These events can be viewed on the server configuration, Alerts definitions, Defined events property page. Information that displays includes the Event name, Description, and Component (LCU represents License Manager) associated with the event. Three of these events—listed in the table that follows—allow you to set criteria thresholds.




You must have *Modify* or *Create* permission in Access policies in order to set compliance event thresholds

<i>Event name</i>	<i>Explanation</i>
Software installed approaching purchased licenses	The percentage of the number of software licenses installed to the number of software licenses purchased is at or above the limit specified, as set in the License compliance events thresholds dialog box.
Software installed below minimum	The percentage of the number of software licenses installed to the number of software licenses purchased is at or below the limit specified, as set in the License compliance events thresholds dialog box.
License expiration date approaching	The difference in days between the license expiration date and the current date, as set in the License compliance event thresholds dialog box, is at or below the limit specified.



Events based upon calculated fields, such as percentage, are based on value after rounding. Percentages are rounded to integers and date differences are rounded to integer days.

Recognition of a license compliance event occurs at regularly-scheduled intervals and after relevant license data has been updated from inventory data. An event is fired only once when the event condition is first encountered; however, it will fire again if the condition disappears and then reappears.

To alter default thresholds for license compliance events, click  **Event thresholds** on the button bar. The License compliance event thresholds dialog box appears.

Use the spin buttons to set thresholds for events or enter the values in the fields provided.



If you change an event threshold in the License compliance event thresholds dialog box, then any event that may become applicable due to the change will fire immediately.

Click **OK** to save your thresholds and close the dialog box.



For information on defining alerts that correspond with License Manager events, [“Alert definitions” on page 193.](#)

Patch console

Supported Client types – Windows

You can use the Patch console page to prepare for deploying Microsoft patches over Patch Manager channels. The Patch console page allows you to view live patch information about the patches that Microsoft makes available on their Web site, edit individual patch properties, and select patches for download. You can also use Patch console tools to start the Patch List Synchronization schedule on demand, rather than waiting for the schedule to run according to its defined schedule.



The Patch console requires some setup activity for first-time use. See [“Preparing the patch list” on page 214](#).

Server Configuration > Patch Console

Products	Updates																																																															
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Microsoft <input type="checkbox"/> BizTalk Server <input type="checkbox"/> Compute Cluster Pack <input checked="" type="checkbox"/> Exchange <input type="checkbox"/> Expression <input type="checkbox"/> Forefront <input type="checkbox"/> Internet Security and Acc... <input type="checkbox"/> Microsoft System Center D... <input type="checkbox"/> Office <input type="checkbox"/> Office Communications Ser... <input type="checkbox"/> SDK Components <input type="checkbox"/> Silverlight <input type="checkbox"/> SQL Server <input type="checkbox"/> Systems Management Serv... <input type="checkbox"/> Virtual Server <input type="checkbox"/> Visual Studio <input checked="" type="checkbox"/> Windows 	<table border="1"> <thead> <tr> <th>Update ID</th> <th>Title</th> <th>Classification</th> <th>Downloaded</th> <th>Released</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> 1049965</td> <td>Update Rollup 6 for Excha...</td> <td>Update Rollups</td> <td>N</td> <td>2008-02-21T17:55:...</td> </tr> <tr> <td><input checked="" type="checkbox"/> 1077741</td> <td>Update Rollup 1 for Excha...</td> <td>Update Rollups</td> <td>N</td> <td>2008-03-05T18:00:...</td> </tr> <tr> <td><input checked="" type="checkbox"/> 1271999</td> <td>Update Rollup 2 for Excha...</td> <td>Update Rollups</td> <td>N</td> <td>2008-05-08T00:53:...</td> </tr> <tr> <td><input checked="" type="checkbox"/> 1355876</td> <td>Security Update for Exch...</td> <td>Security Updates</td> <td>N</td> <td>2008-07-08T17:00:...</td> </tr> <tr> <td><input checked="" type="checkbox"/> 1355886</td> <td>Security Update for Exch...</td> <td>Security Updates</td> <td>N</td> <td>2008-07-08T17:00:...</td> </tr> <tr> <td><input checked="" type="checkbox"/> 1355909</td> <td>Update Rollup 3 for Excha...</td> <td>Security Updates</td> <td>N</td> <td>2008-07-08T17:00:...</td> </tr> <tr> <td><input checked="" type="checkbox"/> 1355932</td> <td>Update Rollup 7 for Excha...</td> <td>Security Updates</td> <td>N</td> <td>2008-07-08T17:00:...</td> </tr> <tr> <td><input checked="" type="checkbox"/> 1636070</td> <td>Update for Intelligent Mes...</td> <td>Update Rollups</td> <td>N</td> <td>2008-10-01T17:00:...</td> </tr> </tbody> </table>	Update ID	Title	Classification	Downloaded	Released	<input checked="" type="checkbox"/> 1049965	Update Rollup 6 for Excha...	Update Rollups	N	2008-02-21T17:55:...	<input checked="" type="checkbox"/> 1077741	Update Rollup 1 for Excha...	Update Rollups	N	2008-03-05T18:00:...	<input checked="" type="checkbox"/> 1271999	Update Rollup 2 for Excha...	Update Rollups	N	2008-05-08T00:53:...	<input checked="" type="checkbox"/> 1355876	Security Update for Exch...	Security Updates	N	2008-07-08T17:00:...	<input checked="" type="checkbox"/> 1355886	Security Update for Exch...	Security Updates	N	2008-07-08T17:00:...	<input checked="" type="checkbox"/> 1355909	Update Rollup 3 for Excha...	Security Updates	N	2008-07-08T17:00:...	<input checked="" type="checkbox"/> 1355932	Update Rollup 7 for Excha...	Security Updates	N	2008-07-08T17:00:...	<input checked="" type="checkbox"/> 1636070	Update for Intelligent Mes...	Update Rollups	N	2008-10-01T17:00:...	<table border="1"> <thead> <tr> <th>Detail</th> <th>Security Bulletin</th> <th>KB Article</th> <th>Description</th> <th>More Info</th> <th>EULA</th> <th>CVE</th> </tr> </thead> <tbody> <tr> <td colspan="2">Property</td> <td colspan="5">Description</td> </tr> </tbody> </table>				Detail	Security Bulletin	KB Article	Description	More Info	EULA	CVE	Property		Description				
Update ID	Title	Classification	Downloaded	Released																																																												
<input checked="" type="checkbox"/> 1049965	Update Rollup 6 for Excha...	Update Rollups	N	2008-02-21T17:55:...																																																												
<input checked="" type="checkbox"/> 1077741	Update Rollup 1 for Excha...	Update Rollups	N	2008-03-05T18:00:...																																																												
<input checked="" type="checkbox"/> 1271999	Update Rollup 2 for Excha...	Update Rollups	N	2008-05-08T00:53:...																																																												
<input checked="" type="checkbox"/> 1355876	Security Update for Exch...	Security Updates	N	2008-07-08T17:00:...																																																												
<input checked="" type="checkbox"/> 1355886	Security Update for Exch...	Security Updates	N	2008-07-08T17:00:...																																																												
<input checked="" type="checkbox"/> 1355909	Update Rollup 3 for Excha...	Security Updates	N	2008-07-08T17:00:...																																																												
<input checked="" type="checkbox"/> 1355932	Update Rollup 7 for Excha...	Security Updates	N	2008-07-08T17:00:...																																																												
<input checked="" type="checkbox"/> 1636070	Update for Intelligent Mes...	Update Rollups	N	2008-10-01T17:00:...																																																												
Detail	Security Bulletin	KB Article	Description	More Info	EULA	CVE																																																										
Property		Description																																																														

The Patch console page contains three panes:

- Products pane – The left pane contains a tree structure for product families. Expand, collapse, and select product families that have patches available.
- Updates pane – The top right pane contains the individual patch updates for the product family you select in the product pane.
- Detail pane – The bottom right pane contains the detailed content for the patch you select in the updates pane. All information on the property pages reflects information that Microsoft makes available for the patch. Microsoft does not populate all properties for all patches. The detail pane includes the following property pages:
 - Detail – Several important patch attributes; including severity, identifiers, version number, reboot behavior, and more.
 - Security Bulletin – Live access to the Microsoft TechNet Security Center’s bulletin.

- KB Article – Live access to any related knowledge base article.
- Description – Complete description text.
- More Info – Supplemental information not captured by other property pages.
- EULA – End User Licence Agreement (EULA).
- CVE – Common Vulnerabilities and Exposures (CVE).

The following Afaria activities are for after you prepare the patch list:

- Create Patch Manager channels – Create channels to deploy patches to Clients. See *Afaria Reference Manual | Components, Patch Manager*.
- Use the Data views > Client patches – Use the Client patches data view to query the Afaria database about which Clients have patches installed and take action to deploy patches on Patch Manager channels to the Clients that need them. See [“Viewing client patch information” on page 487](#).

Preparing the patch list

Using the Patch console for the first time requires that you complete the following general preparatory tasks:

- 1 Define the patch download location. See [“Patch Manager” on page 185](#) to define the patch download location.
- 2 Copy MBSA support files for ESD transfer.
- 3 Copy WUA for ESD transfer.
- 4 Update the patch list.

Copy MBSA files for ESD transfer

The Patch Manager component leverages the Microsoft Baseline Security Analyzer (MBSA) technology to implement Patch Manager features. Patch Manager requires that two specific files from any MBSA installation be present in the Electronic Software Delivery (ESD) folder for transfer to the Client.



Server farm administrators must copy the MBSA files to all servers in a server farm.

Deploying the MBSA client files is a required step for collecting relevant patch information from your Clients, and occurs whenever a Client that doesn't have the MBSA files runs any Patch Manager channel. The MBSA client conducts scans to collect patch-related information about the client. The Afaria Server retrieves the patch information during Afaria sessions for the Client patches view to display.

To copy the MBSA files for Afaria Servers:

- 1 Visit the [Afaria third-party component dependency reference page](#), where you will find version information and download instructions for obtaining MBSA.
- 2 Install Microsoft's Baseline Security Analyzer on any computer that you have available. The computer may be an Afaria Server.
- 3 Copy files mbsacli.exe and wusscan.dll from the MBSA installation to the following folder on each Afaria Server you have that is licensed for Patch Manager:

<AfariaInstallDir>\ClientESD\Win32\PatchMgr

Copy WUA for ESD transfer

The Patch Manager component leverages Microsoft's Windows Update Agent (WUA) technology to implement Patch Manager features. Patch Manager requires that the WUA executable file be present in the Electronic Software Delivery (ESD) folder for transfer to the Client.



Server farm administrators must copy the WUA file to all servers in a server farm.

To copy the WUA file for Afaria Servers:

- 1 Visit the [Afaria third-party component dependency reference page](#), where you will find version information and download instructions for obtaining WUA.
- 2 Copy file WindowsUpdateAgent20-x86.exe to the following folder on each Afaria Server you have that is licensed for Patch Manager:
`<AfariaInstallDir>\Data\Channel\Content\PatchManager`

Updating the patch list

The Patch console is empty when you first install Afaria because it has yet to synchronize with the patch information available from the Microsoft Web site. Afaria uses a daily schedule, the Patch List Synchronization schedule, to perform the synchronization. The first synchronization updates just the product family and patch information. Subsequent synchronizations update product family and patch information, and download the patch selections that you save on the Patch console page that are not already downloaded.

You can control when the Patch List Synchronization schedule runs by using any of the following methods:

- Allow the schedule to run according to its defined schedule properties – Requires no additional action.
- Run the schedule on demand from the Patch console page – See [“Run patch list synchronization on demand” on page 219](#).
- Run the schedule on demand from the server schedules page – See [“Server schedules” on page 186](#).



Downloading patches for the first time may take several hours to complete and may make a noticeable impact on system resources. Refreshing your list of existing patches may take a while as well.



You can verify that the download process is complete by viewing the Messages log.

When the first patch list synchronization is complete, you are ready to use the Patch console page to select patches for download.


Select patches for download

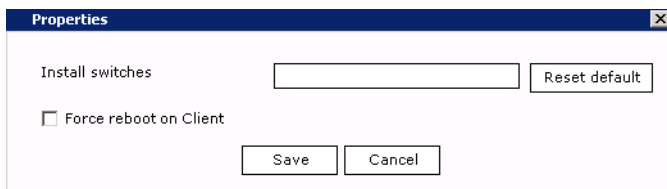
Use the Patch console page to select the patches you want to download, edit any individual patches properties, and save the selection for the next download. Patch properties that you save now are implemented when you use Patch Manager channels to deploy the patches to Afaria Clients.



If you change the switch properties for any patches already associated with published channels, you must use the Channels Administration page's update contents feature to update the contents of any channel associated with the patch in order for any changes to take effect on that channel.

To select patches for download:

- 1 On the global navigation bar, click **Server configuration** and then select **Patch console** on the drop-down menu. The Server configuration, Patch console page opens.
- 2 In the product pane, use the check boxes to select a one or more products. The patches associated with the current product appear in the patches pane.
- 3 In the patches pane, use the check boxes to select the patches you want to download to make them available for Patch Manager channels. You can research any patch by clicking on it and visiting the detail pane.
- 4 (Optional) Edit the switches or download location properties for any selected patch by bringing focus to the patch in the patches pane and click  **Properties** on the toolbar.



The Properties dialog box includes the following data items:

- **Install switches** – Allows you to set the switches that determine how the patch installs on the Client machine. Choose Reset default to restore default values.
- **Force reboot on Client** – Allows you to force the Client to reboot in cases where the applied patch does not cause the Client machine to reboot.

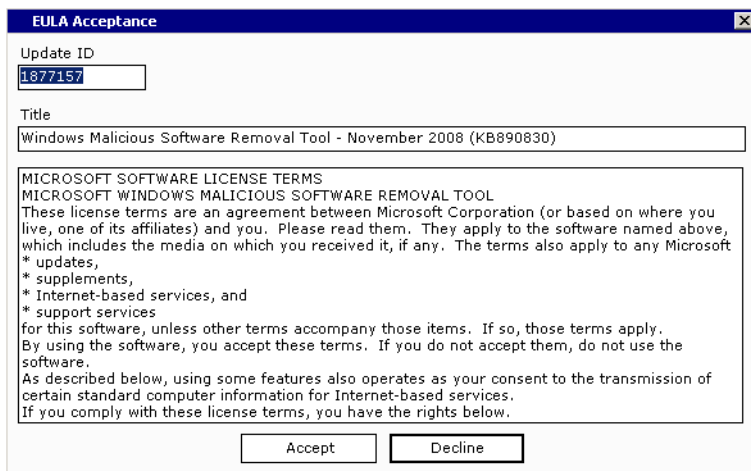
Choose **Save** to save the properties.

- 5 Use the **Save** toolbar icon to save the Patch console page changes. You may be prompted with EULA dialogs.

You are ready to download the selected patches. You can download your patches now or let the patches download the next time the patch list updates according to the Patch List Synchronization schedule.

About the EULA dialogs

Afaria may prompt you with a EULA dialog when you save your patch selections on the Patch console page.



EULA dialog example

Consider the following items when responding to End User License Agreement (EULA) dialogs:

- Each EULA dialog is associated with a single patch. However, not all patches have an associated EULA.
- The EULA statement represents a proposed agreement between your organization and Microsoft.

Your response to the EULA dialog represents your organization's response on behalf of all users that will receive that patch. Individual users are not prompted with a EULA dialog.

Downloading patches for server farms

The Patch List Synchronization schedule runs for only one server at a time. Therefore, configuring all servers in a farm with the same schedule results in only one server downloading the patches.


Consider using recommended practices for managing Patch Manager downloads in server farms:

- Shared patch download location – Configure each server to use the same directory location for patch downloads.
- Run only one synchronization schedule – Configure one server with a Patch List Synchronization schedule to run daily. Configure remaining servers' Patch List Synchronization schedules to run once for a date and time in the past, effectively disabling the schedules.
- Use the Patch console page to select the patches you want to download, edit any individual patches properties, and save the selection for the next download. Patch properties that you save now are implemented when you use Patch Manager channels to deploy the patches to Afaria Clients.

Run patch list synchronization on demand

Use the Patch console page to run the Patch List Synchronization schedule whenever you want. Running the schedule updates the patch list information for all the Microsoft product families and downloads any selected patches on the page that are not already downloaded. Synchronizing and downloading is a resource-intensive process and can be lengthy, so plan accordingly. You may want to avoid running the Patch List Synchronization schedule during peak or near-peak hours.

To run patch list synchronization on demand:

- 1 View or make changes on the Patch console page.
- 2 Save any page changes. You may be prompted with EULA dialogs.
- 3 Click  **Run Schedule** on the toolbar to start the Patch List Synchronization schedules.

Create Patch Manager alerts

You can use the **Server configuration, Alert definition** feature to create alerts to notify you when problems have occurred with downloading patches or executing the Patch List Synchronization schedule. The following events are associated with the Patch Manager component:

- Download failed – *One or more files were not downloaded.* This means you may need to run the Patch List Synchronization schedule again, or try to download the patch manually from the Microsoft site.
- Download needed – *One or more files were deleted during the data synchronization. You must download these files manually.* Some patches that were previously downloaded to your server were deleted when the Patch List Synchronization schedule ran and refreshed the patch list. You should check the Microsoft site to ensure the patch files still exist; if they do, you can download them manually from the Microsoft site.
- Schedule failed – *Error occurred when Patch List Synchronization schedule last ran.* You need to check the Data views, Messages Log to view any errors that may have occurred when the schedule last ran.

See [“Alert definitions” on page 193](#).



Administration

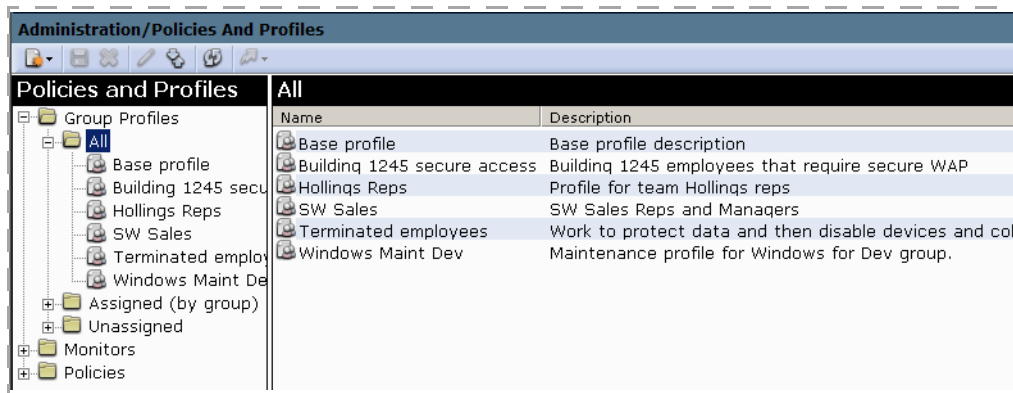
Use the Administration area for day-to-day tasks related to your Afaria solution. The Administration area provides you with tools for managing:

- Profiles
- Policies
- Client groups
- Channels and channel sets
- Channel replication
- Monitors
- OMA DM device definitions

Profiles

Use the Policies and Profiles area of Afaria Administrator to create or manage profiles. In a server farm environment, you can view profiles from any server. However, use the main server to create or edit profiles.

Administration > Policies and Profiles

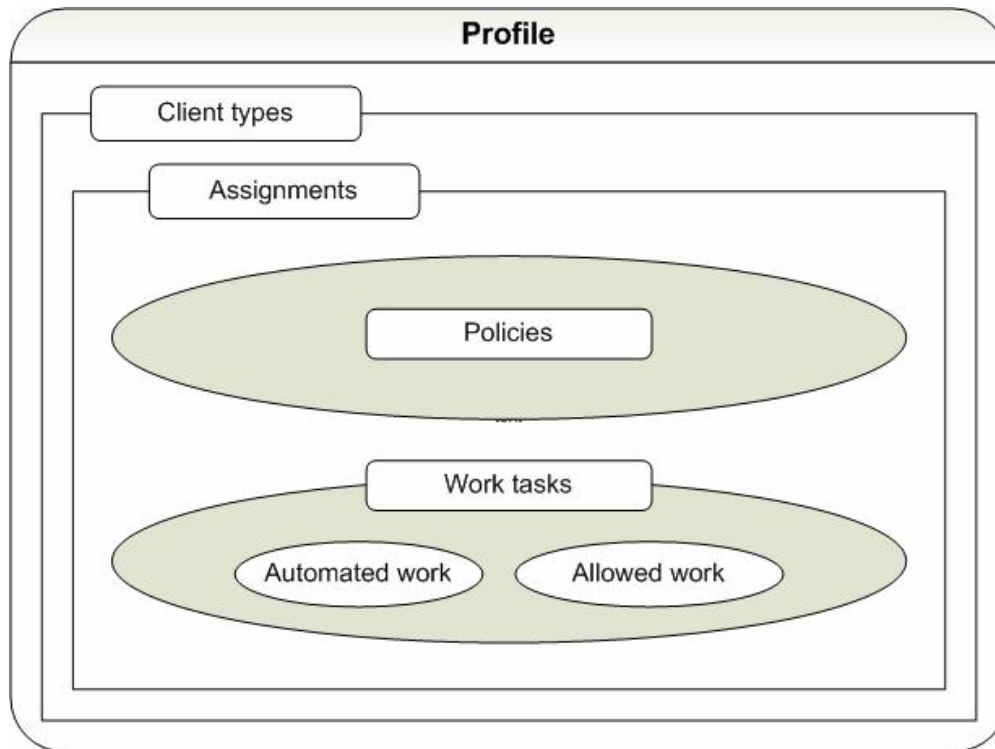


The list in the left pane contains all defined profiles by category:

- All – Contains all profiles.
- Assigned (by group) – Contains all profiles assigned to groups, categorized by group.
- Unassigned – Contains profiles that are not assigned to any groups.

About Profiles

Profiles are the primary mechanism for managing the policies applied to groups, and the work performed by groups. The Afaria administrator creates profiles as vehicles for associating policies and work tasks with groups. Profiles are primarily defined by their client types, assignments, policies, automated work, and allowed work.



Profiles are made up of the following major components:

- Client types – A client type filter defines the types of client devices that can use a profile. For example, you can define a profile to be eligible for all Afaria-supported device types, only one device type, or some combination of multiple device types. Client type and its management implications are further defined in [“Profile – Details” on page 229](#).
- Assignments – Assignments define the list of groups that receive a profile. Groups that are not assigned to a profile do not receive the profile. See [“Profile – Assignments” on page 231](#).
- Policies – Profiles let you apply policies to groups that are enforced either continuously or according to a schedule. See [“Profile – Policies” on page 243](#).
- Automated work – Automated work executes without user interaction. Define monitor-action pairs to automate work. A monitor-action pair is a single schedule or other monitor paired with a single action. The paired action may be to connect to an Afaria Server to request a channel, to launch a program, or some other supported action. See [“Profile – Client Actions” on page 233](#).

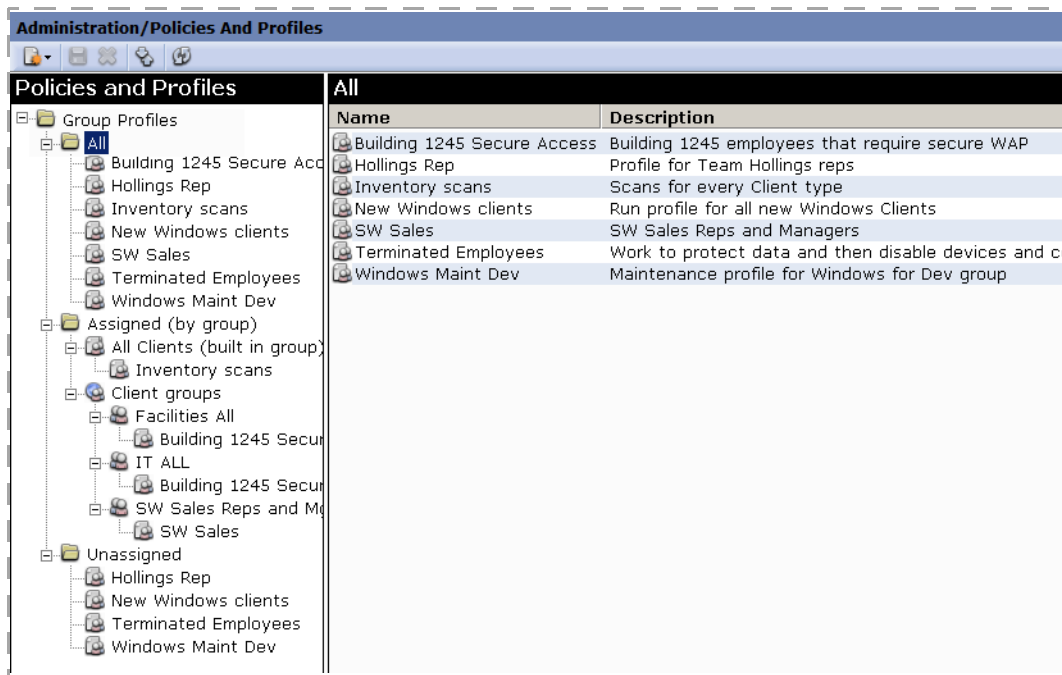
- Allowed work – Allowed work executes when it is requested by a client and is defined as allowed on the profile. Create a list of allowed channels to define the work that the group is allowed to perform. See [“Profile – Allowed Channels” on page 240](#).

A profile’s structure provides flexibility in managing groups.

Managing Profiles

Use the Policies and Profiles page's toolbar and shortcut menus to invoke management commands such as create, delete, and import. Clients are updated with their current profile definitions each time they run a session. Therefore, the client must connect to an Afaria Server to receive an updated profile before it becomes effective on the client.

Administration > Policies and Profiles



Creating, Editing, Copying, and Deleting a Profile

The Policies and Profiles page includes commands to manage your profiles.



- Create – Click **New... > Work profile**. Type a unique name for the profile and an optional description.
- Edit – Select a profile in the left pane and edit contents in the right pane. You can edit the following properties:
 - [“Profile – Details” on page 229](#)
 - [“Profile – Assignments” on page 231](#)
 - [“Profile – Client Actions” on page 233](#)

- [“Profile – Allowed Channels” on page 240](#)

- [“Profile – Policies” on page 243](#)



- Copy – Right-click a profile in the left pane and select **Create copy**. A new copy populates the left pane.



- Delete – Select a profile in the left pane and click the **Delete** icon on the toolbar.

While policies, channels, channel sets, and monitors are associated with profiles, they always remain independent of the profile. That is, a change to a policy, channel, channel set, or monitor is reflected in all the profiles with which it is associated.

Sending outbound notifications

An outbound notification is a set of instructions that is sent from an Afaria server to a client. The instructions tell the client to initiate a connection back to its server to run a session to either request a specific channel or apply its policies.

See [“Outbound Notifications” on page 360](#) for sending notifications.

Importing a Profile



Use the import process to transfer profiles and their associated monitors and policies from one Afaria Server’s export location to a peer server. Importing channels is a separate action you should perform prior to importing a profile.

Launch the import command from the toolbar. Afaria uses an import/export wizard to guide you through the following steps.

- 1 Select the import operation.
- 2 Select the profile file to import. The file extension for profiles is PMX.
- 3 Review the list of policies, profiles, and monitors contained in the import file.
- 4 Review the import results.

Consider the following items when you import profiles:

- An imported profile retains its assignments only when the importing server has matching groups.
- When you import the Default Policies Schedule monitor, it creates a conflict with the existing system’s native Default Policies Schedule monitor and is rejected from the import. Therefore, it is recommended that you do not import the monitor.
- (LDAP domain environments) An imported profile retains all of its LDAP domain assignments, even if the importing environment does not have matching LDAP domains. Use the Assignments tab to remove the LDAP assignments that do not match your environment.

- (Nonmultitenancy) An imported profile retains its channels only when the importing server has matching channels.
- (Multitenancy) An imported profile retains its channels only when the importing server and tenant have matching channels.
- (Multitenancy) An imported profile associates with the importing tenant.

See also, [“About Importing and Exporting Channels” on page 310](#) and [“Channel Replication” on page 345](#).

Exporting a Profile



Use the export process to transfer profiles and their associated monitors and policies from an Afaria Server to an export location. Exporting channels is a separate action.

Launch the export command from the toolbar. Afaria uses an import/export wizard to guide you through the following steps.

- 1 Select the export operation.
- 2 Select the profiles to export.
- 3 Select the associated monitors to export.
- 4 Select the associated policies to export.
- 5 Select a file destination for the export. The file extension for profiles is PMX. The wizard can create a folder or file if it does not exist and prompts for confirmation before overwriting a file.

Consider the following items when you export profiles:

- Profile export does not export group definitions.
- Profile export does not export channels. Use Afaria replication processes and export processes to manage channel definition sharing.

See also, [“About Importing and Exporting Channels” on page 310](#) and [“Channel Replication” on page 345](#).

Import/Export Profile Utility

Afaria includes a command-line utility that you can use to execute profile import and export commands.

Command path: <ServerInstallDir>\bin\

Command: profileimportexport

Using command “profileimportexport” without any parameters or options displays a usage example with an options list.

The same considerations that apply to using the user interface to execute the commands apply to using the utility.

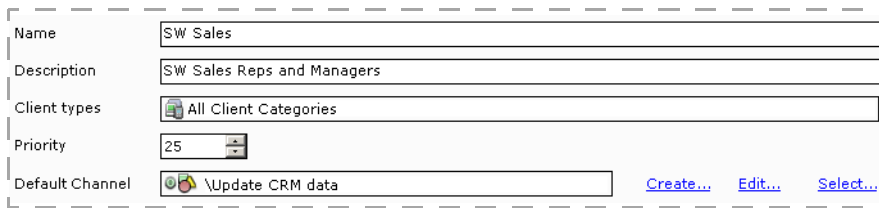
See topics [“Importing a Profile”](#) and [“Exporting a Profile”](#) to review the considerations.

Profile – Details

Use the Details tab to manage basic profile properties, including the default channel value that populates the allowed channels list.

See also “[Profile – Allowed Channels](#)” on page 240.

Administration > Policies and Profiles > *profile*



The screenshot shows a form with the following fields and values:

Name	SW Sales
Description	SW Sales Reps and Managers
Client types	All Client Categories
Priority	25
Default Channel	\Update CRM data

Below the Default Channel field, there are three links: [Create...](#), [Edit...](#), and [Select...](#)

A profile's basic attributes include the following data elements:

- Name – User-defined name.
- Description – Optional description.
- Client types – Filters the types of client devices that are eligible to receive the profile. Define the filter to allow one or more client types. Use the **Edit...** link to select client categories. Use this filter in conjunction with a profile's assignments to determine which clients receive the profile.
- Priority – User-defined value that Afaria uses to determine which profile prevails when multiple profiles define the same default channel. The lower the numeric value, the higher the priority. A high priority prevails over a lower priority.

Priority field ties are resolved using a repeatable, system-defined methodology. The priority value does not relate to any other profile tabs.

- Default channel – Channel or channel set to run for a connecting client that meets all of the following conditions:
 - (User-initiated connection) Client does not have a channel specified in its Afaria configuration settings
 - (API client) Client has an empty string for its channel name parameter

The default channel populates the allowed channels list (“[Profile – Allowed Channels](#)”).

Consider the following items about using the default channel data element:

- 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.
- A client can run only one default channel or one default channel set per session.
- In the case of a client that has multiple profile default channels, see the work profiles' priority values to determine which default channel runs.

- In the case of a client meeting the conditions for running a default channel but without any profile default channels, the following actions take place:
 - Windows clients – Update profile data at the client and update the channel listing in the Channel Viewer.
 - Handheld clients – Update profile data at the client. If the client is also a Document Manager Client, then also update the Document Manager list.

The Details tab displays the following controls for the Default Channel box:

- **Create** – Launch the wizard for creating a new channel or channel set. The wizard begins with a Folder selection dialog to select the new item's location on the Channel Administration page. The wizard continues and finishes with the same wizards you use from the Channels Administration page. See [“Creating a Channel” on page 304](#) and [“Creating and Managing Channel Sets” on page 306](#) for additional instructions.



The channel/set name must be unique. The wizard does not validate the name until the end of the wizard.

- **Edit** – Launch the editor for the channel or channel set.
- **Select** – Launch the Channel selection dialog box to select a channel or channel set.
- **Remove** – Delete the item from the field.

Profile – Assignments

Use the Assignments tab to assign the profile to specific groups. Groups are first filtered by the client types attribute (“[Profile – Details](#)”), then by the Assignments properties.

The Afaria Server does not send a profile to any group until it is assigned. Once assigned, the assigned groups’ clients receive the profile during their next session.

While groups’ clients may receive a profile, each client must meet any channel requirements in order to be able to run the channels. See “[Channel Administration](#)” on page 290 for more information about managing channels. Similarly, a client receives monitor-action pair definitions from the client actions list only when the client type supports the monitor type. See “[Profile – Client Actions](#)” on page 233 and “[Monitor Support by Client Type](#)” on page 319 for more information about clients receiving monitor-action pair definitions.

Administration > Policies and Profiles > *profile* > Assignments

Location	Groups	Description
AFARIAW2K3R2	AfariaAdministrators	Afaria Web Administrator group
Client groups	Sales SW All	Sales SW reps and managers
	Sales NW All	Sales NW reps and managers

The Assignments tab displays the following data elements:

- Location – Location for the group’s definition. You can assign profiles to the following types of groups:
 - Afaria client groups
 - Afaria built-in group “All Clients”

The All Clients group is a dynamic group that includes every known client. Using the group simplifies assigning a profile to all clients. This group is used only in the policies and profiles user interface. It is not exposed in the **Administration > Client groups** user interface.

Windows Mobile Professional, Windows Mobile Standard – The Create Client Installation program can seed client packages with schedules and other supported monitors if its associated profile includes the All Clients group assignment. See “[Schedule Monitor Deployment Considerations](#)” on page 343 for additional information.

- LDAP user groups, as supported by the Afaria system requirements



See “[Channels – Security Tab](#)” on page 296 for information about the importance of using channel authentication with user group assignments.

- Local user groups
- Domain user groups
- Groups – User- or system-defined group name.
- Description – User- or system-defined group description.

Managing Assignments

Click the **Assign...** or **Remove** links on the Assignments tab to manage assignments on the list. Select a group and click **Members...** to show the individual members of a group.

Clicking **Assign...** opens the Assign groups to profile dialog box.

Administration > Policies and Profiles > *profile* > Assignments > Assign



Move groups from the “Select groups...” list to the “Groups assigned...” list to assign them to a profile. Click **Add >>** and **<< Remove** links to move groups between the lists. Select a group and click **Members...** to show the individual members of the group. Click **Reset tree** to reset the navigation tree in the “Select groups...” list.



LDAP groups – The API that Afaria uses to query for LDAP groups is limited to displaying 1,000 results. Therefore to ensure that any groups you want to use display in your query, add the groups of interest to a custom OU and name so that it is returned in the first 1,000 results of the query.

Profile – Client Actions

Use the Client actions tab to review and manage the monitor-action pairs that are included with a profile.

Monitors are deployed to clients to monitor and detect specific events, such as the existence of a network connection or an instance of a running process. Schedules are also defined as monitors. Monitors that detect their associated event can then initiate their paired action, such as run a channel or create a log entry.

See [“Channel Administration” on page 290](#) for detailed information about creating channels and channel sets. See [“Monitors” on page 316](#) for detailed information about monitors.

Administration > Policies and Profiles > *profile* > Client actions

Enabled	Monitor	Monitor type	Action type	Channel name	Action definition
<input checked="" type="checkbox"/>	Power_225	Power Monitor	Log Event Only		Power 225 event
<input checked="" type="checkbox"/>	Power_225	Power Monitor	Run Script		stopprocesses.js -l-d
<input checked="" type="checkbox"/>	WAP secure bldg 1245	Schedule Monitor	Run Channel	ConfigMgr - WM	AFARIAW2K3R2\ConfigMgr
<input checked="" type="checkbox"/>	WAP secure bldg 1245	Schedule Monitor	Log Event Only		Building

The Client actions list includes the profile’s monitor-action pairs. The page displays the following data elements:

- Enabled – Defines whether the monitor-action pair is enabled within the profile. Afaria sends only active monitors to clients.
- Monitor – User-defined monitor name.
- Monitor type – System-defined monitor type.
- Action type – System-defined action type.
- Channel name – Channel or channel set name.
- Action definition – The nature of the content in the action definition column varies depending on the action type but always includes some significant data element from the action definition, such as channel name or logged message.

Managing Client Actions

Click the **Add...** or **Edit...** or **Remove** links on the Client actions tab to manage monitor-action pairs on the list. Choosing **Add...** or **Edit...** launches the Client Action Editor.



The system manages monitor-action pair Default Policies Schedule-Apply Policies. It is associated with the presence or absence of specific policy types.

Administration > Policies and Profiles > *profile* > Client actions > Add...

A screenshot of the Client Action Editor form, enclosed in a dashed border. It contains two input fields: "Monitor" with an empty text box and "Action type" with a dropdown menu showing "Select action type". To the right of the "Monitor" field are three blue, underlined buttons: "Create...", "Edit...", and "Select...".

The Client Action Editor includes all the features you need to create, edit, or select the elements for your monitor-action pair. Each pair requires one monitor and one action type. The following are eligible action types:

- Log event only
- Execute program
- Run channel
- Run script

Action type "Apply Policies" is reserved for system use.

Action Support by Client Type

Although actions are not device-specific, feature availability depends on client type features and platform support. For this reason, actions may function differently or not at all on different client types.

Any action is eligible to become part of a monitor-action pair. However, it is your responsibility to understand which actions are valid for which client types. See the following table to learn about action support by client type.

	Action type	Log event only	Execute program	Run channel	Run script
	Windows	X	X	X	X
Client type ^a	Windows Mobile Professional	X	X	X	X
	Windows Mobile Standard	X	X	X	X
	Symbian			X	
	BlackBerry			X	

a. Palm and Java devices do not support monitors and therefore, are not eligible for monitor-action pair assignment.

Defining the Monitor in a Monitor-Action Pair

Any monitor is eligible to become part of a monitor-action pair. However, it is your responsibility to understand which monitors and monitor features are valid for which client types. See [“Monitor Support by Client Type” on page 319](#).

The Client Action Editor includes the following monitor controls:

- **Create** – Launches the monitor wizard to guide you through selecting a monitor type and defining its attributes. The monitor type list is filtered to display only those monitors that are supported by the profile’s client types ([“Profile – Details”](#)).



The filtering of the type list is a usability aid, not a substitute for understanding which monitors are valid for which client types.

- **Edit** – Launches the monitor editor. Changes you make to the monitor affect all of the its associated profiles.
- **Select** – Opens Monitor Selection dialog box. Select a monitor from the list.

Defining the “Log Event Only” Action

The “Log event only” action lets you collect data from the monitor event. The data is transferred to the server’s Client Triggered Actions log during the next connection.

The action includes the following data element:

Additional text – Text to include with the event’s log entry.

Defining the “Execute Program” Action

The “Execute Program” action lets you specify a program file to execute with any associated command line parameters. The program must already exist on the client.

The action includes the following data elements:

- Program name – Program’s file name.
- Parameters – Any parameters for executing the program.
 - Enclose individual parameters in quotation marks if the parameter includes a space.
 - Delimit multiple parameters with a single space.
 - Monitor substitution variables are valid parameters. However, they must not be enclosed in quotation marks. Syntax example: <MonitorData1>. See [“Monitor Substitution Variables” on page 319](#) and individual monitor topics for addition information about the variables.
- Wait for completion, Criteria, Retries – See [“Common Action Attributes” on page 238](#).

Defining the “Run Channel” Action

The “Run Channel” action lets you specify a channel or channel set to run. A channel must be published to run, but may in an unpublished state when you define your monitor-action pair.

The action includes the following data elements:

- Channel name – Name of the channel or channel set to run.
- Wait for completion, Criteria, Retries – See [“Common Action Attributes” on page 238](#).

The Client Action Editor includes the following “Run Channel” action controls:

- **Create** – Launch the wizard for creating a new channel or channel set. The wizard begins with a Folder selection dialog to select the new item’s location in on the Channel Administration page. The wizard continues and finishes with the same wizards you use from

the Channels Administration page. See [“Creating a Channel” on page 304](#) and [“Creating and Managing Channel Sets” on page 306](#) for additional instructions.



- The channel/set name must be unique within the “save as” target folder. The wizard, as executed from the Client Action Editor, does not validate the name until the end of the wizard.
 - All available channels are listed in the wizard. It is your responsibility to understand which channels are valid for which client types.
- **Edit** – Launch the editor for the channel or channel set.
 - **Select** – Launch the Channel selection dialog box to select a channel or channel set.

Defining the “Run Script” Action

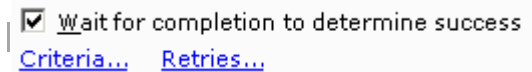
The “Run Script” action lets you specify a JScript or VBScript to execute on the client. The script must already exist on the client in the root folder.

The action includes the following data elements:

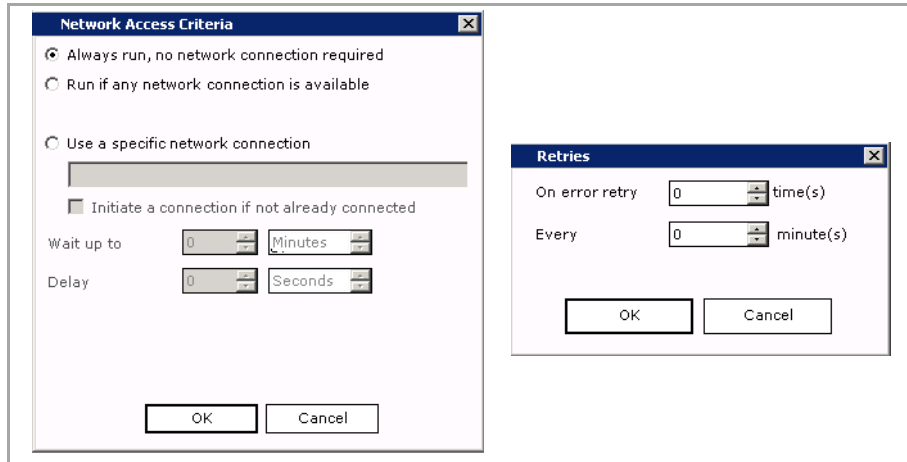
- Script name – File name of the script, including the script file’s extension.
- Script function name – (Case-sensitive) Script function name to call for execution.
- Parameters – Any parameters for executing the script.
 - Enclose individual parameters in quotation marks.
 - Delimit multiple parameters with a single space.
 - Monitor substitution variables are valid parameters. However, they must not be enclosed in quotation marks. Syntax example: `<MonitorData1>`. See [“Monitor Substitution Variables” on page 319](#) and individual monitor topics for addition information about the variables.
- **Wait for completion, Criteria, Retries** – See [“Common Action Attributes”](#).

Common Action Attributes

The Client Action Editor includes some of the same action attributes on multiple action types.



...profile > Client actions > Client Action Editor > attributes



- **Wait for completion to determine success** – Determines whether or not Afaria waits for the action to complete before logging it. If the Retries feature is also used, then Afaria logs only the final success or failure. You cannot clear the check box if retry values are currently defined; you must reset retry values to zero.
 - **Retries** – Determines the number of times and the frequency in minutes for retrying a failed action. Afaria cancels any pending retries if action has cause to execute again, such as the case of a schedule monitor with repeat settings causing the event to occur again.
- **Criteria** – Specify whether the action runs based on network parameters for the client connecting to the server.
 - **Always run, no network selection required** – This option executes the action regardless of the client's connectivity state. If a connection is required but is not available, an attempted session will fail.
 - **Run if any network connection is available** – This option executes the action only if network connectivity is already established. Afaria does not end the connection upon session completion. If connectivity is not already established, the action is not executed but may be attempted again at the next instance of the monitor's event.
 - **Use a specific network connection** – This option executes the action only if a named network connection is already established. If connectivity is not already established, the action is not executed but may be attempted again at the next instance of the monitor's event.

You can select the **Initiate connection if not already connected** option to enable clients to start a connection.

Client Action Execution

Monitors execute their associated action when the defined monitor criteria is met. However if the associated action cannot be completed at that time—due to connection criteria or error retries—and the monitor process is terminated for any reason, then the action never completes and is never be logged.

Client Action Logging

Actions performed on clients are logged on the Afaria Server and have logging policy properties and log cleanup properties. See [“Logging policy” on page 135](#) for information on how to set client action logging services policies, and [“Log cleanup” on page 138](#) for information on cleaning up and deleting client action logs.

Profile – Allowed Channels

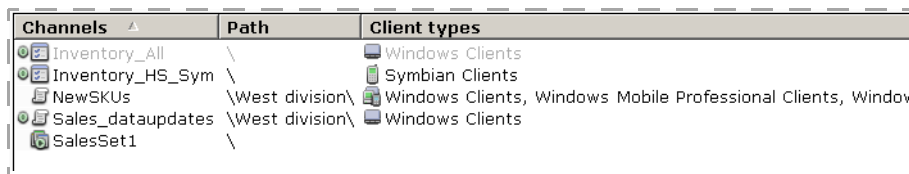
Use the Allowed channels tab to review and manage the channels and channel sets that a profile’s assigned groups are allowed to run.

While groups’ clients may receive a profile that includes allowed channels, each client still must meet any channel requirements in order to be able to run the channels. See “[Channel Administration](#)” on page 290 for more information about channels.

Allowed channels are requested by clients in a variety of ways, including the following examples:

- Scheduled connection – A client makes a scheduled connection after its schedule monitor prompts its associated run channel action to execute.
- Windows client with Channel Viewer – A user selects the channel’s name in the Channel Viewer application and issues the connect command.
- Windows client or handheld client – Client opens the channel’s parameter file (.XEC).
- API client – A client runs a session using the channel’s name as the channel parameter.
- Monitor-action pair – A run channel action executes, as defined by a monitor-action pair that used a connection monitor to detect an active connection.
- Default channel – A client’s Afaria configuration settings do not define any channel when the client is connecting.

Administration > Policies and Profiles > *profile* > Allowed channels



Channels	Path	Client types
Inventory_All	\	Windows Clients
Inventory_HS_Sym	\	Symbian Clients
NewSKUs	\West division\	Windows Clients, Windows Mobile Professional Clients, Window
Sales_dataupdates	\West division\	Windows Clients
SalesSet1	\	

The Allowed channels tab displays the following data elements:

- Channels – Name for the channel or channel set.
- Path – Path for the defined channel or channel set, as it exists on the Channels Administration page.
- Client types – Channels only. Lists client types selected for the channel.

The Allowed channels tab displays the following controls:

- **Create** – Launch the wizard for creating a new channel or channel set. The wizard begins with a Folder selection dialog to select the new item’s location on the Channel Administration page. The wizard continues and finishes with the same wizards you use from

the Channels Administration page. See [“Creating a Channel” on page 304](#) and [“Creating and Managing Channel Sets” on page 306](#) for additional instructions.



The channel/set name must be unique within the “save as” target folder. The wizard, as executed from the Client Action Editor, does not validate the name until the end of the wizard.

- **Edit** – Launch the editor for the channel or channel set.
- **Select** – Launch the Channel selection dialog box to select an existing channel or channel set.
- **Remove** – Delete the item from the list. The item remains defined on the Channels Administration page.
 - **Remove** is enabled only for list members that you added by using the **Create** or **Select** controls.
 - Using the Remove control does not delete the channel from the list if the channel is also the default channel or a defined action on the profile. You can remove persistent members by ensuring they are no longer the default channel nor a defined action.

Consider the following items about channels and channel sets on the allowed channels list:

- Channel requirements – Having channels on the allowed channels list does not mean that clients can run the channels unconditionally. Each client that requests a channel must meet any channel requirements in order to be able to run the channel.
- Channels vs. channel sets – You must add an individual channel from a channel set to the list if you want the channel to be allowed in any context other than as a member of a set.
- Requesting channel sets – When a client requests a channel set, the client attempts to run each channel in the set; each channel is run or not run based on how the client is evaluated against the channel’s properties. Client-side messages may open on the client to notify the user about instances when a channel is not run.
- Document Manager – Document Manager channels are designed to require user interaction at the client. Due to the user interaction that makes them useful, Document Manager channels must always be included on the allowed channels list. For Windows Channel Viewer users, the channel must also include the visibility attribute.
- How items are added to the list – The Allowed channels list may include items added by the following methods:
 - Items are added to the list by using the **Create...** or **Select...** controls on the Allowed channels tab. Items display in black. You can remove these items by using the **Remove** control.
 - Items are added to the list by either their status as the default channel on the profile’s Other options tab or by their status as a defined action on the profile’s Client actions tab. Items display in gray. You can remove these items by ensuring they are no longer the default channel nor a defined action.
- About removing items from the list – A handheld client requesting a channel that was on its profile’s allowed channels list but has been removed, is left in an undesirable state: its channel request will be denied and it will be unable to receive an updated profile. It will remain in that state until it can make one of the following requests:

- Request a channel from its allowed channels list – You can restore the removed channel to the profile or have the user change the Afaria Client configuration's channel setting to request a channel from the allowed channels list.
- Request a blank channel – You can have the user delete the Afaria Client configuration's channel setting. Connecting to request a blank channel causes the Afaria Server to run the client's default channel (see ["Profile – Details" on page 229](#)).

Profile – Policies

Use the Policies tab to review and manage the policies that a profile's assigned groups enforce. Policies let you create focused collections of settings and tasks to define and enforce on your clients. Policies are applied at the client during every session and according to the schedule associated with the Default Policies Schedule monitor-action pair.

While a groups' clients may receive a profile that includes policies, each client must meet any policy requirements to be able to apply the policies. See [“Policies” on page 247](#).

Administration > Policies and Profiles > *profile* > Policies

Enabled	Policy	Policy type	Client types
<input checked="" type="checkbox"/>	Spam block	AntiVirus policy	Windows Mobile Professional, Symt
<input checked="" type="checkbox"/>	Install address book	OMA DM Policy	OMA DM
<input checked="" type="checkbox"/>	Setting Access for WM Pro	Settings Access Policy	Windows Mobile Professional
<input checked="" type="checkbox"/>	General for WM Pro	General Configuration Pt	Windows Mobile Professional
<input checked="" type="checkbox"/>	Access point for corporate	OMA DM Policy	OMA DM

The Policies tab displays the following data elements:

- **Enabled** – Whether or not the policy is enabled within the profile. Afaria enforces only enabled policies. Disabling a policy leaves any client-side components in place on the client but suspends policy enforcement.
- **Policy** – User-defined name.
- **Policy type** – System-defined type.
- **Client types** – Client types defined for the policy.

The Policies tab displays the following controls:

- **Create** – Launch an editor to create a new policy and add it to the list. The editor is the same editor from the Policies and Profiles page. See [“Creating, Editing, Copying, and Deleting a Policy” on page 248](#).
- **Edit** – Launch the editor for the selected policy.
- **Select** – Select an existing policy. If the policy is the first one of its type for a receiving client, then any client-side components associated with the policy type are installed on the client, regardless of whether you choose to enable the policy.
- **Remove** – Delete the item from the list. If the policy is the last-remaining policy of its type on a client, then remove the policy and remove any client-side components associated with the policy type from client and terminate policy management on the device. The item remains defined on the Afaria Administrator's list of policies, as viewed on the Policies and Profiles page.

Group Profile Examples

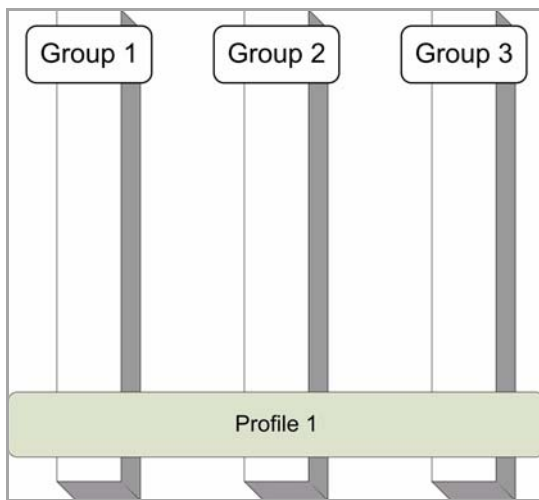
The tremendous flexibility afforded by the profile design provides many ways for you to implement a profile strategy for your organization.

The following examples provide sample implementations. The groups and profiles depicted in the diagrams represent a subset of an organization's groups and profiles. The samples are intended only to present ideas; they are not intended to define a "right" or "wrong" implementation, nor are they intended to define a comprehensive set of possible implementations.

As you consider the examples, bear in mind that groups can either be based on your organization's defined user groups, defined Afaria client groups, or a combination of group types. See "[Profile – Assignments](#)" on page 231 for more information about group assignments.

Example 1

Work is the same for all groups or is differentiated for groups at the channel level by using channel properties for client type or channel security. Consider the following possible scenarios.



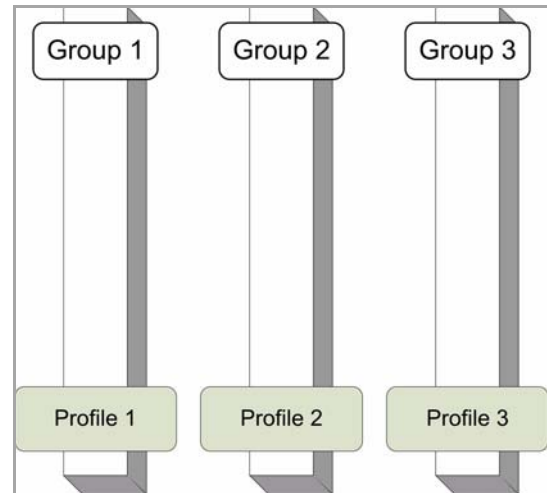
- All client connections for various client types are initiated from custom applications using client API calls. A profile captures all the called channels or channel sets in the profile's allowed channels list.
 - Group 1 – Afaria client group for Windows laptop computers.
 - Group 2 – Network user group
 - Profile 1 – Profile is available to all client types. The Assignments includes the system-defined "All Clients" group. The allowed channels list is populated with all of the channels that the clients call.
- All clients are Windows clients that run without the Channel Viewer application. Connections are driven by client actions. The profile defines a list of monitor-action pairs for which

running a channel or channel set is the defined action. A channel set may contain a number of channels that define all the work for the clients.

Example 2

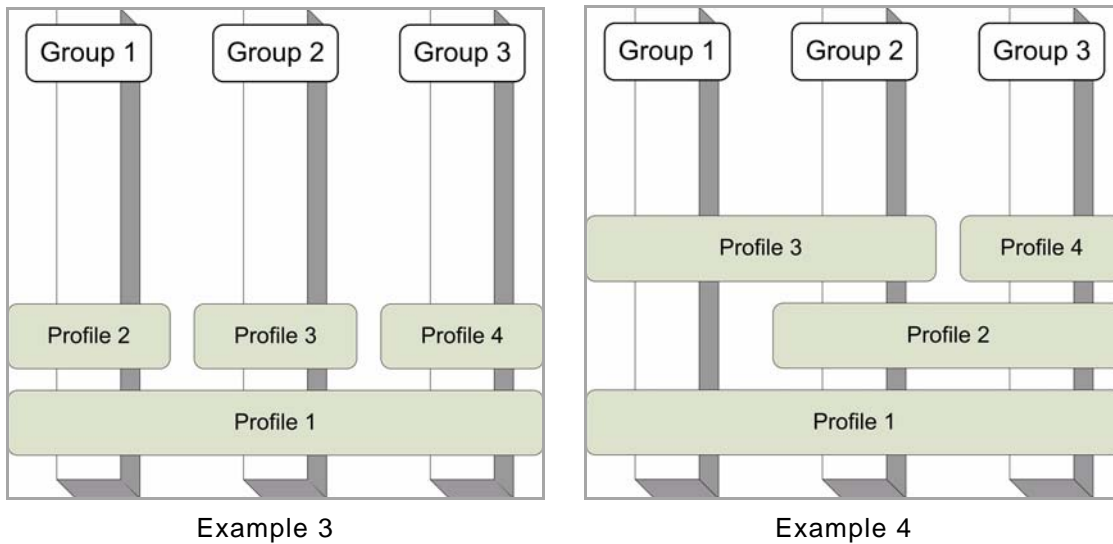
Work may be the same or different for the groups. However, using the profile's assignments properties lets you manage the work separately for separate groups. Consider the following possible scenarios:

- The groups are user groups: executives, IT personnel, and general users. Each group has different Afaria work based on their personal role in the organization. The Afaria work might include software and document distribution for all, differentiated by personal roles.
- The groups are client groups. Each group has similar Afaria work, differentiated by client device capabilities. The Afaria work might include device configuration and security policies.



Examples 3 and 4

The profile strategies are hybrids of the previous examples. Groups share some work and have some differentiation.



Consider the following scenarios:

- Example 3 – Inventory scanning and backup management is the same for all client types and user groups and is captured into a shared profile. Remaining work is divided into separate profiles, each with different connection schedules.
- Example 4 – A profile that is shared across all groups includes work to push an organization's common documents and announcements to all clients, respective of client type. Additional profiles include work to pull back specific documents from the different groups that each group is responsible for updating.

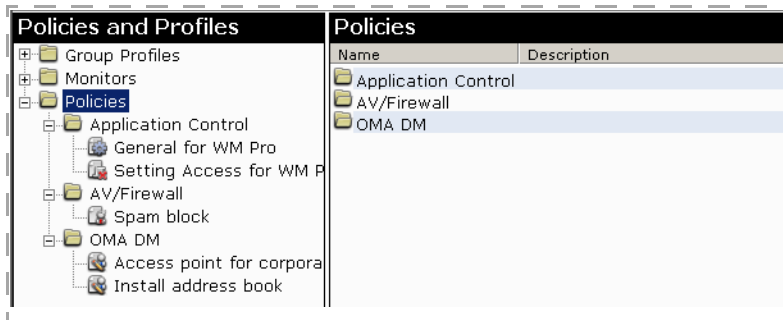
Policies

Use the Policies area of Afaria Administrator to define and manage policies. Policies let you create focused collections of tasks and actions to define and enforce on your clients.

Group Profiles and Policies

Profiles are the vehicles for distributing policies to client devices; policies are components in the profile's definition. Include policies with profiles, on the profile's policies list, to associate them with Afaria Clients or OMA DM Clients. See ["About Profiles" on page 223](#).

Administration > Policies and Profiles



Managing Policies

Use the Policies and Profiles page to invoke management commands such as create, delete, and import. In a server farm environment, you can view policies from any server. However, use the main server to create or edit policies.

Creating, Editing, Copying, and Deleting a Policy

The Policies and Profiles page includes commands to manage your policies.

- Create – Click **New...** > **Policy type** to open a policy editor. Use only alphanumeric characters to define the user name. Define the remaining policy settings according to its policy category.
 - [“Policy Category – Application Control” on page 250](#)
 - [“Policy Category – Antivirus/Firewall” on page 255](#)
 - [“Policy Category – OMA DM” on page 259](#)
- Edit – Select a policy in the left pane and choose the **Edit** link in the right pane to open the policy editor. Edit the policy according to its policy category.
- Copy – Right-click a policy in the left pane and select **Create copy**.
- (Multitenancy) Copy to another tenant – Right-click a policy in the left pane and select **Copy to Tenant**, select a target tenant, and click **OK**.
- Delete – Select a policy in the left pane and click the **Delete** icon on the toolbar.

Any change to a policy is reflected in all the profiles with which it is associated.

Sending outbound notifications

An outbound notification is a set of instructions that is sent from an Afaria server to a client. The instructions tell the client to initiate a connection back to its server to run a session to either request a specific channel or apply its policies.

See [“Outbound Notifications” on page 360](#) for sending notifications.

Exporting and Importing a Policy

Export and import features are available as part of the profile export and import feature. See [“Importing a Profile” on page 226](#) and [“Exporting a Profile” on page 227](#).

Sending an Outbound Notification to Apply Policies

Send an outbound notification to immediately apply a policy to clients. The outbound notification sends a message to its associated clients, and instructs the clients to start a session with their server. The clients then initiate a connection to the server to receive their policies.

- 1 Select a policy in the left pane.
- 2 Right-click and select **Outbound Notification > Apply Policies**.

The client receives all available profile and policy updates at connection time.

Policy Category – Application Control

Supported client types – Windows Mobile Professional and Windows Mobile Standard

Application control policies let you control which applications your device users can execute. The policies manage different types of applications:

- Embedded applications – Applications that come preinstalled on the device.
- Installed applications – Applications that are installed on your device after purchase.
- Settings menu applications – Applications that are available on the device's Settings menu. Controlling these settings is often critical to device management, as they may control sensitive areas of device functionality.

Policy management compiles a client application library. The library is a list of applications that are on your client devices, as queried by a client-side agent and reported back to the server. It is a reference for your use when defining policies.

Application control workflows:

- [“Preparing for application control policy management” on page 251](#)
- [“Allowing or restricting applications” on page 252](#)
- [“Discontinuing application control policies” on page 254](#)

About the client application library

The client application library lists the applications that are installed on the client's device. Consider these general items about the client application library:

- The library is a single list that lists the embedded, installed, and settings access applications on your devices..



Some applications may appear as both embedded applications and installed applications on a device. They are listed in the library, may be listed in other libraries, and must be managed consistently.

- Populate the library by creating a policy, deploying it to a representative set of clients, and connecting the clients a second time.
- Once the library is populated, select items from the library when you create enforcement policies.
- The library is dynamic. An application control agent on each client scans daily for new applications and reports those applications back to the server.

About the application control agent

Application control policies rely on a single application control agent running on the device to enforce the policy and query for applications. The agent is deployed to the client the first time any application control policy type is deployed to the client. The agent queries the device for applications upon deployment, and then scans the device daily for any new applications. It reports known applications to the server during sessions.

One agent supports all application control policy types. Disabling a policy leaves the agent in place on the client but suspends policy enforcement. The agent is removed from the client when its last application control policy is removed, rather than disabled, from its collective group profiles.

Preparing for application control policy management

Prepare for management before defining policies that allow or restrict applications. The preparation deploys the application control agent to clients and builds the client application library on the server to make it available for future policies.

For multitenancy users, complete this process for each tenant.

- 1 For each client type you plan to support, create a policy. It is a best practice to start with the General Configuration policy, which neither allows nor restricts applications – See [“Creating a general configuration policy” on page 251](#).
- 2 Add each policy to a group profile – See [“Profile – Policies” on page 243](#).
- 3 Deploy the profile to clients – The policy deploys the agent when the client connects. The agent queries its client for applications.
- 4 Connect clients again – The application list is reported to the server and compiled into a single, shared library for the client type.

The library is now available for use in policy editors.

Creating a general configuration policy

Create a general configuration policy to define settings for optional logging. Logging captures information in the Handheld Security logs about user attempts to execute restricted applications.

You can also use a general configuration policy to compile your application library.

- 1 Select **Policies** and right-click **New...> Application Control...> General Configuration**.
- 2 Enter a **Name** and **Description**.
- 3 Select a **client type**.
- 4 (Optional) Select the appropriate logging:

- Installed Application Logging
 - Embedded Application Logging
 - Settings Access Logging
- 5 Click the **Save** icon. The name of the general configuration policy appears in the left pane.
 - 6 Close the editor window.

Allowing or restricting applications

An application control policy allows or restricts applications, depending on the application control policy type.

Prerequisite: Build the client application library. See [“Preparing for application control policy management” on page 251](#).

- 1 Create one or more application control policy types to control your application types:
 - Embedded applications policy
 - Installed applications policy
 - Settings menu applications policy
- 2 Add policies to group profile.
- 3 Deploy profile to clients – Profiles deploy to clients when they connect to the server.

See also:

- [“Creating an embedded applications policy” on page 252](#)
- [“Creating an installed applications policy” on page 253](#)
- [“Creating a settings menu applications policy” on page 253](#)
- [“Profile – Policies” on page 243](#)

Creating an embedded applications policy

Create an embedded application policy to define a list of restricted applications that users cannot run from the application library list. You can log the denied application events in the general configuration policy editor. See [“Creating a general configuration policy” on page 251](#).

- 1 Select **Policies** and right-click **New...> Application Control...> Embedded Applications**.
- 2 Enter a **Name** and **Description**.
- 3 Select a **client type**.
- 4 Define the list of applications. The default allows all applications to run. Perform the following:

- **Select** – Open the client application library to choose the applications to be restricted. The library lists all the applications that come installed on the device.
 - **Add** – Enter applications manually.
- 5 Click the **Save** icon.
 - 6 Click the **Save** icon again. The name of the application control policy appears in the left pane.
 - 7 Close the editor window.

Creating an installed applications policy

Create an installed application policy to define a list of installed applications that you want to allow your users to run from the application library list. You can log denied application events in the general configuration policy editor. See [“Creating a general configuration policy” on page 251](#).

- 1 Select **Policies** and right-click **New...> Application Control...> Installed Applications**.
- 2 Enter a **Name** and **Description**.
- 3 Select a **client type**.
- 4 Define the list of applications. The default restricts all installed applications from running. Perform the following:
 - **Select** – Open the client application library to choose the applications both by the application name or grouped by its certificate that are allowed to run. The library lists the applications both by the application name and grouped by its certificate.
 - **Add** – Enter applications manually.
- 5 Click the **Save** icon.
- 6 Click the **Save** icon again. The name of the application control policy appears in the left pane.
- 7 Close the editor window.

Creating a settings menu applications policy

Create a settings menu application policy to define a list of settings menu applications that users cannot run from the application library list. You can log denied application events in the general configuration policy editor. See [“Creating a general configuration policy” on page 251](#).

- 1 Select **Policies** and right-click **New...> Application Control...> Settings Access**.
- 2 Enter a **Name** and **Description**.
- 3 Select a **client type**.

4 Choose **Select** to open the client application library:

- **Show all** – Lists all applications.
(For Windows Mobile Standard) A GUID or a number may listed as an application and may be changed to a friendly name. When changed, it is displayed with square brackets, for example [phone], where “phone” is the friendly name. It can be undone by clearing the name.

If a name is changed it may affect pre-existing policies that when opened for editing or viewing will display a message similar to... "Policy has been automatically modified to reflect changes in the library view." You will need to save the policy to retain the changes.

- **Consolidated View** – (For Windows Mobile Standard) Consolidates like applications for the client. The number of consolidated applications are indicated by a number in a bracket following the application, for example phone[n], where “phone” is the application and [n] is the number of settings which were consolidated. Changes in the library view, by consolidation, does not change the organization, only the presentation of that information.
- 5 Select the options that are restricted from running on the device. The default allows all applications to run.
- 6 Click the **Save** icon.
- 7 Click the **Save** icon again. The name of the application control policy appears in the left pane.

Close the editor window.

Discontinuing application control policies

Discontinue policies that you no longer want to operate on a client.

- Delete a policy from Application Control – Deleting a policy from an Application Control page removes it from all associated group profiles.
- Disable a policy in a group profile – Disabling a policy leaves the agent in place on the client but suspends policy enforcement.
- Remove a policy from a group profile – If the policy is the last-remaining policy on a client, then removing the policy removes the agent from client and terminates all application control management on the device.

See also [“Profile – Policies” on page 243](#).

Policy Category – Antivirus/Firewall

Supported client types – Windows Mobile Professional, Symbian, Windows Mobile Standard

Antivirus Firewall (AV/F) policies allow you to control and provide security for your device, and to restrict calls and SMS messages to a device. Policies are placed on the document server as part of a group profile and are passed to connected clients.

Antivirus Firewall policies include the following policy types:

- Antivirus policy – Protect and safeguard devices from viruses.
- Firewall policy– Establish a firewall for each device to guarantee its integrity.
- Call Filtering policy – Block incoming calls, block incoming SMS messages, or both.

AV/Firewall workflows:

- [“Preparing for Antivirus Firewall policy management” on page 255](#)
- [“Discontinuing Antivirus Firewall policies” on page 256.](#)

Preparing for Antivirus Firewall policy management

The Antivirus Firewall policy configures the update server for policies to run. It triggers connections to the update server for AntiVirus client updates and new AntiVirus pattern files.

- 1 Configure the server properties for the new client or pattern files:
 - Select **Server configuration ...> Properties ...> AV/Firewall.**
 - Select either “Hold for administrator approval” or “Automatically send to client on next connection” for the updated client files and new pattern files.
- 2 Create one or more of the AV/Firewall policy types:
 - AntiVirus policies
 - Firewall policies
 - Call Filtering policies
- 3 Add your policy to the group profile.
- 4 Deploy profile to clients – Profiles deploy to clients on a predetermined schedule, or when the clients connect to the server.

See also:

- [“AV/Firewall” on page 169](#)
- [“Server schedules” on page 186](#)
- [“Creating Antivirus policies” on page 256](#)
- [“Creating Firewall policies” on page 257](#)
- [“Creating call filtering policies” on page 258](#)

- [“Profile – Policies” on page 243](#)

Discontinuing Antivirus Firewall policies

To discontinue an Antivirus Firewall policy, perform one:

- Remove the policy from the group profile, which also removes it from the client-side components.
- Disable the policy in the group profile by unselecting **Enabled**.
- Disable the Firewall policy by unselecting **Enable Firewall**.

See [“Profile – Policies” on page 243](#).

Creating Antivirus policies

Creating an Antivirus policy allows you to update and scan Antivirus settings. It lets you enable or disable settings, provides for users to change settings, scan external storage cards, and distribute virus pattern files.

To create an Antivirus policy:

- 1 Select **Policies...>** right-click **Policies...>** **New...>** **AV/Firewall...>** **AntiVirus policy**.
- 2 Enter a **Name** and **Description**.
- 3 Enter the **Client types**.
- 4 If you do not select **Enable AntiVirus scanning**, all of the settings are dimmed, which indicates they are inactive, and are not part of the current policy. You may want to use this option to set scanning and pattern files for future policies that are in the planning stage and not active.
- 5 If you select **Enable AntiVirus scanning**, You can specify any or all of these options as part of your policy:
 - Allow users to change settings – Users may change the settings. If enabled, negates any selection for the “Scan external storage cards” option.
 - Scan external storage cards – Allows scanning of external device cards. If enabled, the “Allow users to change settings” option must be unchecked, otherwise the selection is negated.
 - Distribution of virus pattern files – Server administrators may select:
 - Update immediately via SMS – Contact the client immediately via SMS, which may incur charges.
 - Update at next connection – Allow the server to update the client device when connected.
 - Scan Now – Requests each client to start a scan immediately, which may incur charges.
- 6 Click **Save**.
- 7 Close the editor window.

Creating Firewall policies

Create a Firewall policy to define a list of firewall rules. You can add, enable, and disable rules from the predefined firewall rules list. Additionally, you can designate rules that apply to specific IP/ports.

To create a Firewall policy:

- 1 Select **Policies...** > right-click **Policies...** > **New...** > **AV/Firewall...** > **Firewall policy.**
- 2 Enter a **Name** and **Description.**
- 3 Enter the **Client types.**
- 4 If you do not Select **Enable firewall** all of the settings are dimmed, which indicates they are inactive, and are not part of the current policy. You may want to use this feature if you are planning Whitelist, Blacklist, and Firewall rules, but are not ready to activate the policy.
- 5 Select **Enable firewall**, to include these settings and updates as part of your policy:
 - **Whitelist** – Blocks unknown addresses. This is more secure than allowing unknown connections. The rules list defines known connections and designates each as allowed or blocked. To allow an IP/port or range of ports, add it to the list with an “Allow” attribute. To block an IP/port or range of ports, either add it to the list with a “Block” attribute, or leave it off the list.
 - **Blacklist** – Allows unknown addresses. This is less secure than allowing all unknown connections. The rules list defines known connections and designates each as allowed or blocked. To block an IP/port or range of ports, add it to the list with a “Block” attribute. To allow an IP/port or range of ports, either add it to the list with an “Allow” attribute or leave it off the list.
- 6 From the Firewall policy tab select from these options:
 - **Add** – Enter a Firewall rule description, type, direction, IP address, ports and select **OK**, or select **Add New** to add additional rules, or select **Cancel**.

Firewall rules contain:

- Description – Check box (to enable the rule), and name of the Firewall rule (max 25 characters).
 - Type – Allow or block.
 - Dir – Direction in which this rule works; inbound, outbound, or both.
 - IP Addresses – IP addresses, in IPv4 format (including wildcards, example, 192.168.*.*).
 - Ports – A port or a range of ports (0 – 65535).
- **Edit** – To edit a rule, select the rule and select **Edit**. Select **OK** or **Cancel**, when you finish making changes.
 - **Remove** – Select the rule and click **Remove**.
 - **Move Up** or **Move Down** – Select one or more rules, then select **Move Up** or **Move Down** to change the order in which the rules appear.
- 7 Click **Save**.
 - 8 Close the editor window.

Creating call filtering policies

A Call Filtering policy allows you to create and modify a list of call numbers and SMS messages that are blocked. The policy is only for incoming calls, and it allows you to add, edit, and remove call numbers or SMS messages from the list.

To create a Call filtering policy:

- 1 Select **Policies...**> right-click **Policies...**> **New...**> **AV/Firewall...**> **Call Filtering policy**.
- 2 Enter a **Name** and **Description**.
- 3 Enter the **Client types**.
- 4 If you select **Enable call filtering**, the settings and updates are part of the policy; if you leave **Enable call filtering** unselected, call filtering is inactive.
- 5 Select **Allow user changes**, if users are allowed to maintain their own call filter lists.
- 6 Call filtering policy displays the following controls:
 - **Add** – Select and enter the description, phone number, and blocked calls, SMS messages, or both.

Call filtering policy display:
 - Description – Name of the calling number.
 - Number – Phone number or SMS message, 10 digit maximum including special characters.
 - Block – Select Calls, SMS messages, or both.
 - **Edit** – Revise the blocked number or SMS message list and select **OK** or **Cancel**, when you finish making changes.
 - **Remove** – Select the blocked number or SMS message, then click **Remove**, to delete an entry.
- 7 Click **Save**.

Close the editor window.

Policy Category – OMA DM

Open Mobile Alliance (OMA) Device Management (DM) policies are settings and actions for Afaria OMA DM Clients that are based on DM objects, as defined by OMA. The settings and actions that you define using the Afaria OMA DM policy editor are formulated into OMA-DM-compliant message that the Afaria OMA DM server delivers to the client during connections with the client. The policy's content—OMA DM objects—is applied at the client according to each device's OMA DM implementation.

To learn more about OMA DM, visit the Open Mobile Alliance's Web site, www.openmobilealliance.org and search for the Device Management workgroup.

OMA DM policies may include one or more of the following OMA DM tasks:

- Trust – Establish a trusted relationship between the client and the OMA DM server. Trusted relationships let you initiate a client connection to the OMA DM server without prompting for user interaction. See [“OMA DM task – Trust” on page 261](#).
- Access Point (AP) – Configure an access point for network connectivity. See [“OMA DM task – AP” on page 262](#).
- Mail for Exchange (MfE) – Initialize or change the settings for the Mail for Exchange client. MfE is also used to create an MfE profile if one does not exist. See [“OMA DM task – Mail for Exchange \(MfE\)” on page 269](#).
- Session Control – Allow the user to control subsequent tasks in the same policy by setting and interrogating variables, and branching to out-of-sequence tasks. See [“OMA DM task – Session Control” on page 271](#).
- Skinny Client Control Protocol (SCCP) – Configure clients to use the Intellisync Call Connect application with the Cisco Unified Communications Manager product. See [“OMA DM task – SCCP” on page 267](#).
- Software Configuration Management (SCM) – Install, update, or remove software applications at the client. See [“OMA DM task – SCM” on page 272](#).
- Session Initiation Protocol (SIP) – Configure profiles for multimedia communication sessions, such as Internet calls with one or more participants. See [“OMA DM task – SIP” on page 273](#).
- Terminal Security – Allow a trusted OMA DM server to perform additional terminal security activities, on a device, such as Wipe, Lock, Unlock, and Reboot. See [“OMA DM task – Terminal Security” on page 275](#).
- VoiceOverIP – Configure clients to use Internet telephony. See [“OMA DM task – VoiceOverIP” on page 276](#).
- Free-form – Use custom XML to define actions on a device-supported OMA DM object. See [“OMA DM task – Free-form” on page 277](#).

Afaria captures OMA DM session return codes in the Afaria Messages log. See “Messages” on page 440.

Case-sensitivity in the OMA DM task editors

It is beyond the scope of the editor to determine whether a text value that you type, such as a user name for an authentication method, requires case-sensitive comparison to another value defined elsewhere in the client’s environment. Therefore, treat all text entries as case-sensitive.

Task action = Add

For tasks that include an add action, refrain from using the action multiple times on the same client. Instead, use the replace action to deploy changes after an add action has occurred on a device.

Using variables in the OMA DM task editors

Afaria supports variable substitution for some values¹ in the OMA DM task editors. You may want to use substitution when a value for a setting may change, based on the device or end user.

The variable substitution is made on a device-by-device basis during each client’s session with the OMA DM server. The variables are populated by a Visual Basic script that you create, based on a provided template, and the client’s International Mobile Equipment Identity (IMEI) number, as provided during the session by the OMA DM server. For example, you may write a script that calls a database that can retrieve the user’s e-mail address based on knowing the user’s device IMEI number.

The following variables are defined in the script:

- UserLogin – User name
- UserPassword – Password
- UserDefined01 – Reserved for your custom use
- UserDefined02 – Reserved for your custom use
- UserDefined03 – Reserved for your custom use

Using a variable in a task editor

The following general steps define how to use variables in the task editors.

- 1 Update the script template with a custom script. Rename the script to “UserDataLookup.vbs” and verify that it is in the stated directory during session

1. Some task editor values use special characters and therefore do not accept variables.

execution to be referenced during the session. The script template is stored in the Afaria Server directory:

- Script path: <InstallDirectory>/Data/Scripts
 - Script template name: UserDataLookup_.vbs
- 2 Insert a variable into a task editor field using:
%VariableName%
Example: %UserLogin%
 - 3 Connect a client to the OMA DM server.

OMA DM task – Trust

The trust task lets you establish a trust relationship between the client and the OMA DM server. A trust relationship requires a secure connection using HTTPS. After an initial prompt requiring the user to enter the first four digits of the server's HTTPS certificate thumbprint, trust relationships enable users to initiate a client connection to the OMA DM server without prompting for user interaction. You can also add or remove some management control that consists of limiting access to a particular functional area of the device. When a device is in a trusted relationship with an OMA DM server an icon appears on the main screen. When an active background connection is being made, the icon changes. It may be parentheses or an underscore around or under the icon. The editor also allows you to remove a trust relationship which removes the icon.

The editor includes the following items:

- Name and Description – Name and description for the task, which appears in the editor's task list.
- Action – The action to take on the client:
 - Add – An object is added to the device.
 - Remove – An object is removed from the device if it is found.
- Trust – Lists trust management types to add or remove from the device:
 - Device management – Limits access to edit, create, or delete device management profiles available on the device. To indicate that limited access is active, a white "<" symbol or a lock symbol may appear to the right of the profile names. For devices that do not display symbols, you will receive notification that a device is locked when you attempt to edit or delete an object.
 - Access point management – Limits access to edit, create, or access point management profiles available on the device. To indicate that limited access is active, a white "<" symbol or a lock symbol may appear to the right of the profile names. For devices that do not display symbols, you will receive notification that a device is locked when you attempt to edit or delete an object.
 - Wireless LAN management – Limits access to the wireless LAN connection. You can view WLAN connections, but you cannot establish a connection. If a WLAN connection is already configured, it may appear on the available access points list with a white "<" symbol to the right of the WLAN

connection name. For devices that do not display symbols, you will receive notification that a device is locked when you attempt to verify that a WLAN connection is already configured.

- E-mail management – Limits the ability to create a POP3 or IMAP mail profile in the device messaging application. You cannot create a profile. You can delete an existing profile.
- Terminal security management – Allows a trusted OMA DM server to perform additional terminal security activities, such as wipe, lock, unlock, and reboot, on the device.

Trust management requirements

The following items are required to establish a trust relationship between the OMA DM server and client:

- HTTPS communication – The OMA DM server and client must communicate over the HTTPS protocol.
- Certificate support – The OMA DM server and client must each have the appropriate certificates installed. The certificates may be self-signed or from a certificate authority (CA).
 - OMA DM server – The server must have both a trusted root certificate and an HTTPS certificate. Use IIS management support tool httpcfg.exe's "set ssl" action to associate the HTTPS certificate with the server's address and HTTPS port that it uses for client sessions. See your IIS product documentation for detailed instructions.
 - OMA DM Client – The client must have a trusted root certificate. If the server's SSL certificate is from a CA, the root certificate may already be present on the device. If the certificate is self-signed or is not installed, you must install it on the device. The certificate installation can be done in several ways, including via an OMA CP message, a system indicator message, or via a Web link.
- Certificate thumbprint – To establish trust, the OMA DM server must configure security policies on the client. The device prompts the end user to supply the first four digits of the certificate's thumbprint. You must inform the end user of those digits from the OMA DM server's HTTPS certificate prior to the device management session, such as an e-mail message or other notification.

OMA DM task – AP

The Access Point task lets you define a client configuration for using a GPRS or WLAN access point. The client configuration must match your enterprise's network configuration, as defined by the network administrator. Contact your network administrator for information about your enterprise's access points.

The UI in the task editor is configured differently for each connection type:

- GRPS
 - Basic attributes – ["Shared settings – basic attributes" on page 263](#)

- Settings (GPRS) – “Settings (GPRS)” on page 263
- IPv4 – “IPv4” on page 266
- IPv6 – “IPv6” on page 266
- Proxy – “Proxy” on page 267
- WLAN
 - Basic attributes – “Shared settings – basic attributes” on page 263
 - Settings (WLAN) – “Settings (WLAN)” on page 264
 - Security – “Security” on page 264
 - IPv4 – “IPv4” on page 266
 - IPv6 – “IPv6” on page 266
 - Proxy – “Proxy” on page 267

Shared settings – basic attributes

The task’s basic attributes determine the type of access point and whether the task adds, replaces, or removes the object on the client.

The editor includes:

- Name and Description – Name and description for the task that appears in the editor’s task list.
- Action – The action to take on the client:
 - Deliver – Delete the object from the device if it is found. If not found, add the object to the device.
 - Deliver only if object does not exist – Add the object to the device if it is not found.
 - Remove – Remove the object from the device if it is found.
- Settings name – Access point name that appears on the client.
- Access point type – Select GPRS or WLAN.

Settings (GPRS)

The editor for AP type GPRS includes:

- GPRS access point name – Name that the client shows for access point name.
- User name – User name for logging in to the network, if required.
- Password – Password for logging in to the network, if required.
- Allow plain text login – Allow the user name and password to remain decrypted, as determined by your network administrator.

Settings (WLAN)

The editor for AP type WLAN includes the following items. All values are defined by your network's administrator.

- Primary network name – Service-set identifier (SSID) of the primary network. The maximum length for a network name is 32 characters.
- Network operation mode – Defines mode for client-to-client communications:
 - Ad hoc – Clients can communicate directly with each other, without using the WLAN access point.
 - Infrastructure – Clients must use the WLAN access point to communicate with each other or any LAN devices.
- Hidden network – Select if the SSID is hidden in your network.

Security

The editor includes the following items. All values are defined by your network administrator.

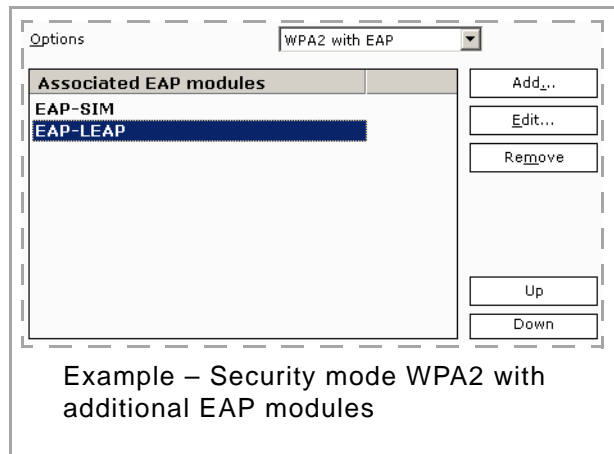
- Options (simple, without EAP modules) – Identify the security mode used by the WLAN in its simplest mode, without using extensible authentication protocol (EAP) modules:
 - Open network – No further settings required.
 - 802.1x – Requires a WPA pre-shared key. Type a passphrase that will get converted into a WPA key for the client.
 - WEP – Identify the key index, authentication mode, and associated WEP keys 1 – 4.
WEP keys 1-4 – Select mode HEX (hexadecimal) or CHAR (alphabetic) and type the passphrase for the key. Represent 64-bit keys as 5 CHAR or 10 HEX characters. Represent 128-bit keys as 13 CHAR or 26 HEX characters. Indicate your intended key length. Extra actual characters, as compared against your indicated key length, are truncated. For example, typing 6 CHAR characters and indicating key length 64 results in truncating the 6th character to yield a 5-character string.
 - WPA and WPA2 – Requires a WPA pre-shared key. Type a passphrase that will get converted into a WPA key for the client.

- Options (with EAP modules) – Identify the security mode used by the WLAN network. Modes may be used with EAP modules. EAP modules add user authentication to the mode's operation.



Afaria supports using the following EAP module types:

- Subscriber Identity Module (SIM)
 - Authentication and Key Agreement (AKA)
 - Lightweight EAP (LEAP)
 - Transport Layer Security (TLS)
 - Tunneled Transport Layer Security (TTLS)
 - Protected EAP (PEAP)
- Security with EAP modules – Choose **Add...** to open the EAP Definition dialog box, which includes all the settings for selecting your EAP module type and defining its values.
 - Edit...** and **Remove** change or remove module definitions.
 - Up** and **Down** determine the order of the modules in the list. The order of the list determines the order of the method that the client uses to attempt to authenticate itself against the network.



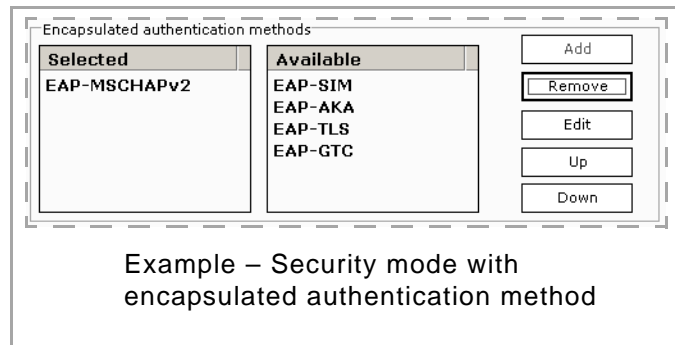
EAP module types PEAP and TTLS support encapsulating authentication methods within their module definition.



Afaria supports encapsulating the following authentication method types:

- Subscriber Identity Module (SIM)
- Authentication and Key Agreement (AKA)
- Transport Layer Security (TLS)
- Microsoft Challenge-Handshake Authentication Protocol v2 (MSCHAPv2)
- Cisco Generic Token Card (GTC)

- Encapsulating authentication methods within an EAP module – Choose **Add...** to open the EAP Encapsulated Definition dialog box, which includes all the settings for selecting your authentication method and defining its values.



- **Edit...** and **Remove** change or remove module definitions.
- **Up** and **Down** determines the order of the modules in the list. The order of the list determines the order of the method that the client uses to attempt to authenticate itself against the network.

IPv4

The editor includes the following items. All values are determined by your network administrator.

- Options – Define the method for mapping device names to IP addresses.
 - Use DHCP – Use the dynamic host configuration protocol (DHCP) to automatically retrieve domain name system (DNS) server addresses.
 - Specify address – Specify a DNS server address, formatted according to the IPv4 standard.
- Specify a DNS server address:
 - IP address
 - Subnet mask
 - Default gateway
 - Primary DNS server
 - Secondary DNS server

IPv6

The editor includes the following items. All values are determined by your network administrator.

- Options – Define the method for mapping device names to IP addresses.
 - Use DHCP – Use the dynamic host configuration protocol (DHCP) to automatically retrieve domain name system (DNS) server addresses.

- Specify address – Specify a DNS server address, formatted according to the IPv6 standard that uses eight groups of four hexadecimal digits. For example: “2453:0db8:85a3:0000:0000:8a2e:0370:2834”.
- Use the following settings to specify a DNS server address:
 - Primary DNS server
 - Secondary DNS server

Proxy

The editor includes the following items. All values are determined by your network administrator.

- Options – Define whether to use a proxy server for routing connections:
 - No proxy – Do not use a proxy server.
 - Specify proxy – Use a proxy server.
- Use the following settings to specify either an HTTP proxy or an HTTPS proxy, but not both:
 - HTTP proxy server
 - HTTP port number
 - HTTPS proxy server
 - HTTPS port number

OMA DM task – SCCP

The Skinny Client Control Protocol (SCCP) task lets you configure clients to use the Intellisync Call Connect application with the Cisco Unified Communications Manager product. The task requires a defined WLAN access point and operational Internet telephony on the client.

The editor includes:

- Basic attributes – [“Basic attributes” on page 268](#)
- Configuration settings – [“Configuration settings” on page 268](#)
- Communication Manager – [“Communication Manager” on page 268](#)
- Release 1.1 settings – [“Release 1.1 settings” on page 269](#)

Basic attributes

The task's basic attributes determine the client's name for its SCCP profile and whether the task adds, replaces, or removes the object on the client.

The editor includes:

- Name and Description – Name and description for the task that appears in the editor's task list.
- Action – The action to take on the client with the policy:
 - Deliver – Delete an existing SCCP if the AP is found. If successful, add a new SCCP.
 - Deliver only if object does not exist – Add the SCCP only if both the AP is found and an existing SCCP is not found.
 - Remove – Remove the object from the device if it is found.
- SCCP profile name – SCCP profile name used at the client.

Configuration settings

The editor includes the following items. All values are determined by your Call Connect and Unified Communications Manager administrator.

- Registration always on – Enable to scan for available WLAN access point and automatically register with Unified Communications Manager.
- Trivial File Transfer Protocol (TFTP) server address configuration mode:
 - Use DHCP – You must have DHCP enabled on the client.
 - Specify address – Specify an associated IP address.
- Call forwarding number in unconditional situations – Global System for Mobile Communications (GSM) number to use for call forwarding when the availability of the call recipient is not verified before making the call.
- Music server address – URL for online music services.
- Voice mailbox number – Call connect voicemail phone number.
- WLAN access point – You can select the "DM Account Activation IAP," or you can manually enter the access point name. The selections available also include any access point defined under Home >Client Deployment > Access Points.
- International Call Prefix – Prefix for making international calls.

Communication Manager

The editor includes the following items. All values are determined by your Call Connect and Unified Communications Manager administrator.

- Cisco Unified Communications Manager Version; syntax is *n.n*, such as "3.5"

- Cisco Unified Communications Manager (1 – 5):
 - Address
 - Port

Release 1.1 settings

The editor includes the following items. All values are determined by your Call Connect and Unified Communications Manager administrator.

- URL for online services – URL for accessing online services.
- Switch to GSM number – Number to use when transferring from an Internet call to a GSM call.
- License key – Call Connect license key.

OMA DM task – Mail for Exchange (MfE)

The Mail for Exchange task initializes or changes the settings required for the operation of the Mail for Exchange client. These settings specify the connection with a Microsoft Exchange Server, user's credentials, schedule for synchronization, data to be synchronized, and that are specific to the email applications. The MfE object cannot be created or removed by OMA DM. It is created when MfE is installed and can be removed only by uninstalling the MfE application.

The editor includes:

- Name and Description – Name and description for the task that appears in the editor's task list.
- Action – Action on the client:
 - Deliver – Object settings are delivered every time the device connects.
 - Deliver only if object does not exist – Object settings are delivered if the exchange server node is not populated.
- Exchange Server and Port – Exchange server and port number of the Microsoft Exchange Server to which the device connects.
- Access Point – Default logical reference to connectivity information. The selections available include any access point defined in Home >Client Deployment > Access Points.
- Synchronization:
 - Use secure connection – Specifies a secure connection (SSL) that is used in synchronization.
 - Conflict resolution – Determines whether the mobile device or the server entries prevail, when a content conflict occurs during synchronization.
 - Sync while roaming – Allows synchronization while roaming.

- Exchange accounts: User name, Password, Confirm password, and Domain – Defines user name, password and domain for the Microsoft Exchange account.
- Sync schedule:
 - Peak sync schedule – Synchronization schedule for peak hours.
 - Off-peak sync schedule – Synchronization schedule for off-peak hours.
 - Peak start and peak end times – Select the start and end time for the peak hours.
 - Peak Days – Select the days that are considered peak days.
 - Heartbeat interval – Interval posted to the server for always-on (ping) jobs. Visible on the device when Peak Schedule = “Always On.” The heartbeat internal value that you set for your device is used as a starting point. You can leave the default value as is. MfE monitors the connection to determine the best setting for your current environment.
- Calendar:
 - Synchronize Calendar – Synchronize the calendar to go back in time a specified amount of time.
 - Sync calendar back – Determines how far back calendar entries are to be synchronized.
 - Delete phone entries on initial sync – During initial synchronization, remove existing entries and replace them with entries from the Microsoft Exchange Server.
- Tasks:
 - Synchronize Tasks – Synchronize tasks and delete phone entries on the initial synchronization.
 - Sync completed tasks – Select “Synchronize completed tasks” or “Do not synchronize tasks.”
 - Delete phone entries on initial sync – During initial synchronization, remove existing entries and replace them with entries from the Microsoft Exchange Server.
- Contacts:
 - Synchronize Contacts – Synchronize contacts and delete phone entries on initial synchronization.
 - Delete phone entries on initial sync – During initial synchronization, remove existing entries and replace them with entries from the Microsoft Exchange Server.
- Email:
 - Synchronize Email – Synchronize and send e-mail messages.
 - E-mail Address – Enter E-mail address of the Microsoft Exchange account.
 - Show new mail popup – Select to display a message each time you receive a new e-mail message.
 - Send mail – Specifies when to send an e-mail message.
 - Sync back – Specifies how far back in time an e-mail message is to be synchronized.
- Signature:
 - Use signature – Selection indicates text is in the Signature field in the e-mail.
 - Signature – Text is included in an e-mail if “Use signature” is selected.

OMA DM task – Session Control

The Session Control task editor allows the user to control subsequent tasks in the same policy by setting and interrogating variables and branching forward (forward only) to out-of-sequence tasks.

The editor includes:

- Name and Description – Name and description for the task that appears in the editor’s task list.
- Possible actions – Action to take on the client:
 - If – Allows two operands, an operator, and compound conditions by entering “or” or “and.”
 - Else, Endif – Statements with no operands.
 - Set – Allows a left operand, which must be a variable, and a right operand that must be a quoted string, a numeric, or a variable.
 - End task, End session, Abort session – Requires no operands.
 - Write to file – Three operands are available:
 - Filename, a fully qualified file name
 - Append, either “yes” or “no”
 - Value, a quoted string or variable
 - Write to session log – Specify a single operand with a message, which may contain variables.
 - Save session logs – Enter either “yes” or “no.”
 - Set session log level – Specify the level of logging detail:
 - Critical = 1
 - FromPolicyTask = 2
 - Important = 3
 - Info = 4
- Left Operand, Operator, Right Operand – The appearance of the fields are dependent on which action is selected:
 - If action – All three fields.
 - If Set – Left and right operands, renamed to “Variable” and “Value.”
 - Write to session log – Only the left operand, renamed to “Message text” and lengthened.
 - Save session logs – “Yes” or “no” using radio buttons.
- Variables – The “variables” listview is visible only for these action codes: *If, Set, and Write to session log.*
- Operations:
 - **Add** – Copy current action and operands and operators to the first empty line in the listview.

- **Edit** – Copy current selected action in the listview to the action field, and operand and operator fields.
- **Replace** – Copy the current action and operands and operators into the selected action of the listview, replacing what is there.
- **Delete** – Delete the current selected action from the listview.
- **Move up** and **Move down** – Move up or down one position to select an action from the listview.

Session control task editor showing several logic statements and task variables.

Action	Operands, expressions, etc
If	%IMEI% EQ 3569885412
If	%company_id% EQ "ACS"
Set	%NextTask% = "Set_AP_to_ACS_Division%"
Else	
Set	%NextTask% = "Set_AP_to_All_Divisions%"
Endif	
Endif	

OMA DM task – SCM

The Software Configuration Management (SCM) task lets you install, update, or remove software applications at the client.

The editor includes:

- Name and Description – Name and description for the task that appears in the editor's task list.
- Action – The action to take on the client with the policy.
 - Install software – Install the application to the device if it is new. The application is always delivered to the device, but it is installed only if it is new.
 - Update software – Update the application on the device if it is found.
 - Remove software – Remove the application from the device if it is found.
- Settings name – Name for the settings used at the client.
- Application:
 - Application name – Application's file name.

- Application version – Application’s version number using user-defined syntax, as appropriate for the application. Use consistent syntax for different versions of the same application. This setting is available only for your use; Afaria does not validate it or use it in any way.

Choose **Add...** to open a browse dialog box to navigate to and select an application. Choose **Remove** to delete the current application from the name box and from all SCM tasks that reference the application.



Use the **Remove** control to remove the application both from the current task editor and from any other SCM task that references the application.

- Drive – Drive letter for installing the application. Syntax is x, such as “e”. “!” means “use any available or default drive.”
- Application language – 2-character ISO language code, as recognized by the client. Code must be in uppercase format. “*” means “use the phone’s default language.”

OMA DM task – SIP

The Session Initiation Protocol (SIP) task lets you configure profiles for multimedia communication sessions, such as Internet calls with one or more participants. The task requires an access point on the client.

The editor includes:

- [“Basic attributes” on page 273](#)
- [“Outbound proxy” on page 274](#)
- [“Registrar server” on page 274](#)

Basic attributes

The task’s basic attributes determine the client’s name for its SIP profile, whether the task adds, replaces, or removes the object on the client, and its general definition.

The editor includes:

- Name and Description – Name and description for the task that appears in the editor’s task list.
- Action – The action to take on the client with the policy:
 - Deliver – Delete an existing SIP if the AP is found. If deletion is successful, add the new SIP.
 - Deliver only if object does not exist – Add the SIP if both the AP is found and a SIP is not found.
 - Remove – Remove the object from the device if it is found.
- SIP settings:
 - SIP profile name – Name for the profile used at the client.

- Service profile – Internet protocol to use for the session—IETF or IMS—as defined by the service provider’s network.
- Public user name – User name, as issued from the service provider. Syntax is *username@domain*, such as “john.smith@company.com” and “+1234567@john.smith@company.com”.
- Internet access point – Access point, as defined on the device. You can select “DM Account Activation IAP,” or you can manually enter the access point name. The selections available also include any access point defined in Home >Client Deployment > Access Points.
- Loose routing – Use the loose proxy routing methodology if you are using RFC-3261-compliant SIP proxy servers. Do not use loose routing with SIP 1.0 proxy servers.
- Activate security negotiation – Enable security negotiation for the SIP profile. The security negotiation must be supported by the destination server.
- Use compression – Enable SIP signalling compression. Compression must be supported by the proxy server. Compression is most commonly used with the IMS Internet protocol.
- Enable always-on registration – Automatically scan for, and register with, the profile’s WLAN access point.

Outbound proxy

The editor includes the following items. All values are determined by your network administrator.

- Outbound proxy server address and port – Server address, formatted as an IP address or a fully-qualified domain name.
- Transport protocol:
 - TCP
 - UDP
 - Auto
- User name, password, and confirm password
- Realm

Registrar server

The editor includes the following items. All values are determined by your network administrator.

- Registrar server address and port – Server address, formatted as an IP address or a fully-qualified domain name.
- Transport protocol:
 - TCP

- UDP
- Auto
- User name, password, and confirm password
- Realm

OMA DM task – Terminal Security

The Terminal Security task allows a trusted OMA DM server to perform additional terminal security activities such as wipe, unlock, lock, and reboot, on a device.

The editor includes:

- Name and Description – Name and description for the task that appears in the editor's task list
- Action – The action to take on the client.
 - Device unlock – All of the device features are enabled.
 - Device lock – Most device features are disabled.



In the OMA DM profile, besides the Server name, Server ID, and Password, an Access Point is required. Failure to provide an access point during device provisioning causes the OMA DM profile to be in the "always ask" mode. When this occurs, the device is locked and the Administrator will not be able to unlock the device using the Device unlock option in the Terminal Security feature.

- Device wipe – Removes device data and all non-permanent data including DM settings, unless they were part of the factory configuration. Device wipe also erases inserted memory card data.
- Device reboot – Restarts the device after the end of the DM session.



After executing device reboot, some devices may be locked immediately. Other devices may have locking delayed and will lock when the autolock period has elapsed.

- Lock Settings:
 - Lock code expiration (days) – Number of days when the lock code expires.
- Lock code entry attempts:
 - Limit attempts – Number of attempts to provide a lock code.
- Lock code change limits:
 - Change tolerance – Maximum number of times a lock code can change.
 - Change interval – Number of times a lock code can change during a given time period.
- Auto Lock Period:

- Max autolock period (minutes) – Maximum time that the device user is allowed to set the autolock period. This setting allows the administrator to put restrictions on the device so that a user cannot set the autolockout period to a large time period.
- Autolock period (minutes) – Elapsed time before a device is locked.
- Lock Code Specification:
 - Lock code and confirm lock code – A character sequence to lock a device. The lock code is not required for Afaria to execute any of the commands (lock, unlock, reset, reboot) on the device.
 - Min and max length – Range of 4 – 255 integers.
 - Include upper and lower letters – Lock code requires uppercase and lowercase letters.
 - Include letters and numbers – Lock code requires both characters and numbers.
 - Disallow two consecutive numbers – Lock code does not allow two consecutive numbers.
 - Max repeated characters – Maximum number of repeated characters that are allowed.
 - History buffer – Validates that the new lock code does not match any previous lock codes.
 - Disallow specific strings – Specifies the lock code strings or substrings that are not allowed. Use a semicolon to separate multiple strings.

OMA DM task – VoiceOverIP

The VoIP task lets you configure clients for using Internet telephony.

The editor includes:

- Name and Description – Name and description for the task that appears in the editor’s task list.
- Action – The action to take on the client with the policy:
 - Deliver – Delete an existing VoIP object if the SCCP or SIP objects are found. When the deletion is successful, add a new VoIP.
 - Deliver only if object does not exist – Add VoIP if both the SCCP or SIP objects, and the VoIP is not found.
 - Remove – Remove the object from the device if it is found.
- Internet telephone profile name – The name of the profile as it appears on the client.
- Handover attenuation – The decibel level at which you want to switch the call to an access point with a stronger signal strength. Use values from -80 dB to -70 dB. For example: “-75”.
- Hysteresis – The increase in signal strength decibels required before switching from one access point to another. Use values from 0 – 10.
- Service profile – The type of communication profile to use for voice, over IP communications, such as SIP.

- Profile name – The name of the service profile to use for voice, over IP communication, such as the SIP profile name, as defined on the device.

OMA DM task – Free-form

The Free-form task lets you supply your own XML code for operating on device-supported OMA DM objects for delivery to the client. The code must comply with the Afaria OMA DM server syntax. The OMA DM server transforms the code into an OMA DM syntax before delivering it to the client.

The editor includes:

- Name and Description – Name and description for the task that appears in the editor's task list.



You cannot retrieve “Lock code” and “Disallow specific strings” settings through the Free-form editor.

Using a NULL value in the Free-form editor may cause unpredictable results.

- Task XML – Type or paste your XML code. The editor does not validate your code; it verifies only that the XML is correctly formed.

A number of predefined actions may be inserted into the task XML area:

- Abort session
- Add
- Comment
- Delete
- End task
- End session
- Exec
- FindFetch
- Get
- Get tree
- Get to variable
- If
- Node
- Node, Value
- Node, value, Format
- Package – This option replaces anything in the XML text box with a standard package shell. The user is warned and allowed to cancel the operation if there is any text in the text box.
- Policy

- Replace
- Save session log
- Set
- Save session log level
- Write to file
- Write to session log
- Auto tag completion – When a leading tag is entered, a matching tag is generated and the cursor is placed between the two tags. Supported tags are:
 - <Package>
 - <Action>
 - <Node>
 - <Value>
 - <Format>
 - <StatusCodeVar>

Variables

Both the free-form editor and the session control editor allow the use of package variables. Package variables are set and tested solely in the OmaDm server, and allow a significant degree of control of the OmaDm session. Package variables are not the same as those discussed on [“Using variables in the OMA DM task editors” on page 260](#), which are set and evaluated during Afaria session manager channel processing.

- A package variable name is an alphanumeric string with a leading and trailing percent sign, with no embedded blanks.
- All variables are initialized to an empty string.
- You can use variables:
 - In the Value element for a Get operation, in which case the variable name is where the retrieved information is stored
 - In the Node text for a Get operation, in which case the variable value becomes the target of the Get operation
 - In the Node text for an Add\Replace\Delete\Exec action, in which case the variable supplies the OmaDm object node name
 - In the Node text for a FindFetch action, in which case the variable receives the value of the FoundResultNode
 - In the Value element for an Add\Replace\Exec action, in which case the variable supplies the data to be put in the OmaDm object node name
 - In the StatusCodeVar element of a Node element, to specify a variable to receive the status code of an operation
 - In the Node text and in the Value element for a Set action

- In the expression in a Conditional Value element
- Variable values are substituted into existing strings in the target fields; for example, “.\AP\APId002\NAPDef\%UserDefined01%\Name” becomes “.\AP\APId002\NAPDef\NapId004\Name” if variable %UserDefined01% = “NapId004”.

There are a number of "built-in" package variables that may be used at runtime:

When a connection is made, the OmaDm server automatically sets up the following variables:

- %IMEI%
- %Manufacturer%
- %Model%
- %VerDTD%
- %VerProtocol%
- %MaxMsgSize%
- %MaxObjSize%
- %CredType%

These correspond to the similarly named nodes in the DevInfo object that the device provides on the initial connection. Other standard variables that the server provides:

- %OmaDmServerAppName% - the name of the Afaria OmaDm server, as specified during installation.
- %PkgCompletionCode% - the value of the completion code for the current package.
- %CurrentPolicyTaskName% - the name of the currently-executing task in the current policy.
- %CurrentPolicyName% - the name of the current policy.
- %NextTask% - this variable controls what task (package) is next selected for execution from the current policy. It is a forward selection only - that is, NextTask may not be set for a task earlier in the policy than the task setting the NextTask variable.

OMA DM Examples

The following three coding examples include combinations of conditions and variables in each expression.

Example #1

If the Name node of SyncML/DMAcc/DMId001 is "RickOma", do a Get_tree on the DevInfo object. If the status code of the Get operation (for SyncML/DMAcc/DMId001/Name) is 200, do a Get_tree on the DevDetail object:

```
<?xml version="1.0" encoding="utf-8"?>  
<Package>  
  <Action action="Get">
```

```
<Node>SyncML/DMAcc/DMLd001/Name
  <Value>%APFriendlyName%</Value>
  <StatusCodeVar>%varstat% </StatusCodeVar>
</Node>
</Action>
<Action action="Conditional" actionmodifier="if">
  <Node>
    <Value> %APFriendlyName% EQ "RickOma" </Value>
  </Node>
</Action>
<Action action="Get" actionmodifier="tree">
  <Node>DevInfo</Node>
</Action>
<Action action="Conditional" actionmodifier="if">
  <Node>
    <Value>%varstat% EQ 200</Value>
  </Node>
</Action>
  <Action action="Get" actionmodifier="tree">
    <Node>DevDetail</Node>
  </Action>
  <Action action="Conditional" actionmodifier="endif">
    <Node></Node>
  </Action>
<Action action="Conditional" actionmodifier="endif">
  <Node></Node>
</Action>
</Package>
```

Example #2

If the AP node named "rickm0330b" exists, and if the "IPAddr" node is "10.24.23.115", change the IPAddr to "10.24.23.110", otherwise, change the IPAddr to "10.24.23.120":


```
<?xml version="1.0" encoding="utf-8"?>
<Package>
  <Action action="FindFetch">
    <Node>%internetAP%
      <FindTargetNode>./AP*/NAPDef*/Name</FindTargetNode>
      <FindTargetValue>rickm0330b</FindTargetValue>
      <FoundResultNode>./AP*/NAPDef*/NAPID</FoundResultNode>
      <StatusCodeVar>%findfetchstatus% </StatusCodeVar>
    </Node>
  </Action>
  <Action action="Conditional" actionmodifier="if">
    <Node>
      <Value> %findfetchstatus% EQ 200 </Value>
    </Node>
  </Action>
  <Action action="Get">
    <Node>%internetAP%/NAPDef
      <Value>%napid%</Value>
    </Node>
  </Action>
  <Action action="Get">
    <Node>%internetAP%/NAPDef/%napid%/IPAddr
      Value>%ipaddr%</Value>
    </Node>
  </Action>
  <Action action="Conditional" actionmodifier="if">
    <Node>
      <Value> %ipaddr% EQ "10.24.23.115" </Value>
    </Node>
  </Action>
  <Action action="Replace">
    <Node> %internetAP%/NAPDef/%napid%/IPAddr
```

```
        <Value>10.24.23.110</Value>
    </Node>
</Action>
<Action action="Conditional" actionmodifier="else">
    <Node></Node>
</Action>
<Action action="Replace">
    <Node> %internetAP%/NAPDef/%napid%/IPAddr
        <Value>10.24.23.120</Value>
    </Node>
</Action>
<Action action="Conditional" actionmodifier="endif">
    <Node></Node>
</Action>
<Action action="Conditional" actionmodifier="endif">
    <Node></Node>
</Action>
</Package>
```

Example #3

Find the AP by the name of "AT&T Internet," and save the ID in the variable "%internetAP%". Then find the DM node for the OmaDm server (using the built-in variable "%OmaDmServerAppName%," and save the ID in the variable "%dmID%". If both of these items are found (based on the status code), set the DM object's ConRef node to the initially identified AP node.

```
<?xml version="1.0" encoding="utf-8"?>
<Package>
    <Action action="FindFetch">
        <Node>%internetAP%
    <FindTargetNode>./AP*/NAPDef*/Name</FindTargetNode>
        <FindTargetValue>AT&amp;T Internet</FindTargetValue>
        <FoundResultNode>./AP*/NAPDef*/NAPID</FoundResultNode>
        <StatusCodeVar>%internetfindfetchstatus% </StatusCodeVar>
```

```
</Node>
</Action>
<Action action="FindFetch">
  <Node>%dmID%
  <FindTargetNode>SyncML/DMAcc/*/ServerId</FindTargetNode>
    <FindTargetValue>%OmaDmServerAppName%</FindTargetValue>
    <FoundResultNode>SyncML/DMAcc/*</FoundResultNode>
    <StatusCodeVar>%dmfindfetchstatus% </StatusCodeVar>
  </Node>
</Action>
<Action action="Conditional" actionmodifier="if">
  <Node>
    <Value> %internetfindfetchstatus% EQ 200 AND %dmfindfetchstatus% EQ 200 </Value>
  </Node>
</Action>
<Action action="Replace">
  <Node>SyncML/DMAcc/%dmID%/ConRef
  <Value>%internetAP%</Value>
  </Node>
</Action>
<Action action="Conditional" actionmodifier="endif">
  <Node></Node>
</Action>
</Package>
```

Client Groups

From the Client groups area, you can create Client groups that function similarly to Windows user groups. Client groups contain members based on device types, so you can assign group profiles by device, rather than assigning them to particular users or group. For example, you can create a group of Windows Mobile Standard Clients running at a specific operating system level, and assign the group to a profile containing items to target all the Client devices in that group.

Administration > Client Groups

The screenshot shows the 'Administration/Client groups' window. On the left is a tree view under 'Client groups' containing 'Div1_Dev', 'Div1_Doc', 'Sales NW All', and 'Sales SW All'. The 'Div1_Dev' group is selected. The right pane displays a table with the following data:

Client	Client Type	Client GUID
AFARIAW2K3R2	Windows	{B8524B47-2BBA-41E2-86B6-C4499C914D4C}
AFARIAW2K3R2	Windows	{549B3F52-DA82-F44B-BD5C-931E8330F24D}
AGXPSP3	Windows	{5611DE3A-30B4-48C3-A9F5-9899C1832F67}
AGXPSP3	Windows	{6BAB7E1C-55AF-D847-9CDE-753C4E76DC0A}
CJUNIUS_XP	Windows	{8F7A1307-86EB-914B-8DD1-9F459CCACBA0}
CJUNIUS_XP	Windows	{5FAB4B75-DB24-4A7A-A279-EFB3A844D0A0}
ENGWIN2K3VM	Windows	{7D17BFD6-4D1C-4BDF-A166-5AD93B07D4A9}
WM_Administrat8	Windows Mobile Pr...	{4187D5E8-3762-A7A2-426D-3A436CB2CD75}
XP-BLDG-1245-1	Windows	{AAB4367A-7D7D-4CE8-8F90-7783840BB702}
XP-BLDG-1245-1	Windows	{E75DC3B7-A05B-014A-9F1D-E6AADF088EF9}

In the left pane, a tree structure lists all the Client groups you have defined on your server. When you select Client groups, the following columns appear in the right pane and display the following information about all Client groups on your server:

- Group name – The name you have given the group.
- Group type – One of two types, Dynamic or Static. Dynamic group membership is based on the results of a defined query of the Client database and can change, while static group membership is based on a manual selection of Clients and is static until you change the selection.
- Description – The user-defined description.
- Number of members – The number of members in the group. For static groups, this number does not change unless you edit the group.
- Last update – The last time the group member list was refreshed. This applies mainly to dynamic groups, although the field also shows the date of the last edit for any static group.

If you select a Client group in the left pane, this information appears in the right pane:

- Client name – The name of the Client device.
- Client type – The Client device type, as defined in [“Client types” on page 189](#).
- Client GUID – The unique identifier for each device. Afaria Clients are identified by device GUIDs that begin and end with braces “{” and “}”. OMA DM Clients are typically identified by their IMEI number, without any enclosing braces.

Create a Client group

Create Client groups based on queries that you run through Data views, Clients.



For more information on creating these queries, see “Manage Client data” in the Data views chapter.

Using these queries, you can create two types of Client groups, dynamic and static:

- **Dynamic groups** – For Afaria Clients only. Dynamic groups reference a query created in the View editor in Data Views, Clients and Inventory. For example, you might create a Client view called Symbian Marketing that returns information about all Symbian Clients carried by the Marketing team. In Client groups, you can create a dynamic group that has all Clients returned as part of that query as its members. So if the query returns Symbian 1, Symbian 2, and Symbian 3, each of these Clients is a member of the group. When the query runs again and detects Symbian 4, this member is added to the Client group automatically.

When you click the Refresh icon on the toolbar, a refresh mechanism periodically re-runs the queries, so data is never stagnant.

- **Static groups** – For Afaria Clients and OMA DM Clients. Static groups contain only the members you select from the list of all Client views. For example, you might create a Client view that returns information about all Windows Clients with less than a certain threshold of available hard disk space. In Client groups, you can create a static group that has only specific Clients from that view. The list of members does not change unless you edit it.



For more information about creating Client views, “Creating a Custom Client View” on page 432.

Server Configuration > Clients Groups > New

To create a group, click the **New** icon on the toolbar, or right-click a Client group in the left pane and select **New**. The first page of the Create group wizard appears.

Provide a **Name** and optional **Description** for the group, then select the group type, **Dynamic** or **Static**.

Create group wizard - group type

Select the type of group to create.

Name
Windows - Sales

Description
Sales clients running Windows

Select the group type
Dynamic groups reference a view created by the View editor. These groups contain the views resulting members.

Dynamic

Static groups are created by selecting one or more members from the list of all machines. Group members are constant.

Static

Next> Cancel

Dynamic groups

Supported Client types – Afaria Clients

Server Configuration > Clients Groups > New > Dynamic

Selecting Dynamic on the Create group wizard's first page opens the Dynamic group properties dialog box, which displays the group name and optional description for this group.



To rename a Client group, in the left pane of the Client groups window, right-click the group you want to rename and select **Rename**.

Each view contains a list based on the Client views defined on your server.

Click **Create new Client view** to open the View editor dialog box and create a new view.

You use View editor dialog box to create and manage Client views. Any view you create here also appears in Data views, Clients. See [“Creating a Custom Client View”](#) on page 432.

Click **Finish**. The dynamic group you created appears in the left pane of the Client groups page.

Create group wizard - Dynamic group properties

Name	Description
Windows - Sales	Sales clients running Windows

Select a view

- Client views
 - User Defined Data
 - All Clients
- Client type
 - BlackBerry
 - Windows Mobile Standard
 - Palm
 - Windows
 - Windows Mobile Professional
 - Symbian
- Approved status
 - Approved Clients
 - Unapproved Clients
- Inventory
 - Custom Views

View description

[Create new client view...](#)

Finish Cancel

Static groups

Server Configuration > Clients Groups > New > Static

Selecting Static on the Create group wizard's first page opens the Static group properties dialog box. It displays the group name and optional description for this group.



Rename the Client group by right-clicking the group in the left pane and selecting **Rename**.

Select a group from the All Available Clients box and click **Add** to make it a member of the group. To delete a member from the group, select a Client from the All Available Clients box and click **Remove**.

If a Client does not appear in the All Available Clients box, either click **More data** to repopulate the list, or enter the Client name in the Find Client box and click **Find Client**.

Click **Finish**. The group you created appears in the left pane of the Client groups page.

Create group wizard - Static group properties

Name
WM-Professional - Sales

Description
Sales Clients running WM Professional

All available Clients

Client	Client Type	Clie...
ENGWIN2K3VM	Windows	{7D...
XP-BLDG-1245-1	Windows	{AA...
XP-BLDG-1245-1	Windows	{E7...
WM_Administrat8	Windows Mobile Pr...	{41...
CJUN	Windows	{8F...
CJUN	Windows	{5F...
AFARIAW2K3R2	Windows	{8B...
AFARIAW2K3R2	Windows	{54...
AGXPSP3	Windows	{56...
AGXPSP3	Windows	{6B...

Retrieved 10\10 rows

Find Client

Add >>

<< Remove

Currently selected Clients

Client	Client Type	Clie...
--------	-------------	---------

Retrieved 0\0 rows

Edit or view group properties

Edit groups by selecting a group in the left pane and clicking **Edit** on the toolbar, or by right-clicking the group and selecting **Edit**. The properties dialog box for the group type opens; the fields correspond exactly to the fields on the Static and Dynamic dialog boxes in the Create group wizard. Make any changes and click **OK** to save your edits and close the dialog box.

Administration > Client Groups > group > Properties

View groups by selecting a group in the left pane and clicking **Properties** on the toolbar, or right-clicking and selecting **Properties**.

The Group properties dialog box displays the following Group Name and Group Properties:

- Type – Group type, Dynamic or Static.
- Description – Description entered (if any) when the group was created.
- Number of Members – Number of Client devices in the group; for Dynamic groups, this number may change periodically.
- Last Update – Date and time of any edits or changes to this group. For example, if you are viewing a Dynamic Client group, this may display the date and time a new member of the group was added based on the query results.
- Query Name – Name of the View editor query on which this Client group is based.
- Query – The parameters of the query created in the View editor on which this Client group is based. You cannot edit the query from this dialog box.

Property	Value
Type	Dynamic
Description	
Number Of Members	10
Last Update	12/3/2008 12:00:56 AM
Query Name	All Clients
Query	select ClientName as "Client", A_V_CLIEN...



For more information about creating Client views, ["Creating a Custom Client View" on page 432](#).

You cannot edit any of the fields on this dialog box. Click **Close** to return to the Client groups page.

Delete any group by selecting it in the left pane and clicking **Delete** on the toolbar.

Managing and sending outbound notifications

An outbound notification is a set of instructions that is sent from an Afaria server to a client. The instructions tell the client to initiate a connection back to its server to run a session to either request a specific channel or apply its policies.

See [“Outbound Notifications” on page 360](#) for managing and sending notifications.

Channel Administration

Supported client types – Afaria clients

Use the Channel Administration area to create, edit, and publish channels and channel sets for Afaria clients. Channels are work tasks in the Afaria solution. You can also import and export channels to and from other Afaria Servers in your system.

Group Profiles and Channels



Profiles are the vehicles for distributing channel and channel set tasks to client devices; channels and channel sets are components in the profile's definition. Include channels and channel sets with profiles, either via a profile's Client actions list, or its allowed channels list, or both in some cases in order to associate them with Afaria Clients. See ["About Profiles" on page 223](#) for more information.













Administration > Channel Administration



Channel Administration Icons

The left pane includes a navigation tree for the Afaria Server channel folders, individual channels, and channel sets.

Icon	Description
	Server. The server is the starting point of contact in your system. Each server contains a hierarchical collection of folders, channels, and channel sets. Clients connect to a server to access the server's channels.
	Folder. Use folders to organize channels, channel sets, and other folders.

Icon	Description
	Backup Manager channel. Backs up and restores data from clients.
	Configuration Manager channel. Configure properties on clients.
	Data Protection Manager channel. Provide password protection, data encryption, and enforces specific security settings on clients.
	Document Manager channel. A repository of documents to which client users can subscribe.
	Inventory Manager channel. Perform inventory scans on clients and retrieve detailed data, such as processor type, amount of memory, operating system installed, and commercial software used.
	Patch Manager channel. Deploy security patches and critical updates to minimize security risks and reduce the costs of keeping remote and mobile machines up to date with the latest security patches.
	Server Listing channel. List of other servers to which Channel Viewer users can connect.
	Session Manager channel. Performs system management tasks based on logic and script-like commands that you define. Tasks can execute actions such as directory and file management, system registry, and file distribution.
	Software Manager channel. Delivers and installs software on clients.
	Channel set. You can add individual published channels to a channel set so that all channels in the channel set execute automatically when clients connect.
	Working copy. A duplicate of an original channel. Use a working copy of a published channel when you want to modify a channel but your original channel cannot be changed or unpublished for editing or testing. A (w) at the end of the channel name also indicates that a channel is a working copy of the original. This feature is not available for Session Manager channels.
	Published channel. A channel that you have made available to client users. A published channel cannot be edited unless you first unpublish it or create a working copy.

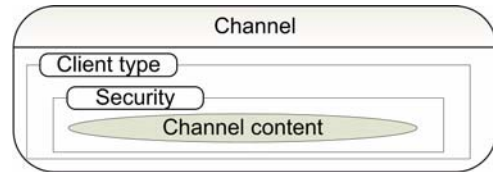
The right pane displays properties for your current selection on the navigation tree. Different tabs are available depending upon the item you've selected in the left pane.

- [“Channels – Properties Tab” on page 294](#)
- [“Channels – Security Tab” on page 296](#)
- [“Channels – Channels Tab” on page 298](#)
- [“Channels – Profiles Tab” on page 300](#)
- [“Channels – HTML Tab” on page 301](#)

Channel and Channel Set Components

Channels are made up of the following major components.

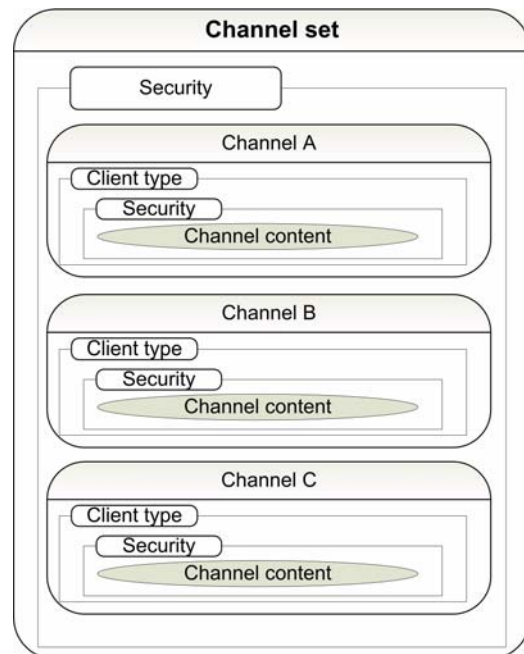
- Client type filter – A client type filter defines the types of devices that can use the channel.
- Security – Security properties provide access safeguards such as user authentication, password protection, and encryption.
- Content – Content is a general term for the channel's definition and the work that the channel causes the client to execute.



The multiple layers of a channel's definition allow Afaria administrators flexibility in building client work.

Channels sets are made up of the following major components.

- Security – Security properties provide access safeguards such as password protection.
- Channels – A channel set contains one or more channels.



Running Channels or Channel Sets on Windows Clients

Afaria supports using the following options for running channels at a Windows client.

- Device- or user-initiated connection
 - Channel Viewer UI – Windows client users access channels from a Channel Viewer application that runs on their client. When you publish a channel and Channel Viewer users connect to the server, channels appear in the Channel Viewer interface.

- Browser UI – You publish channels on a Web page and your Windows client users access the channels using a Web browser. See [“Channels – HTML Tab” on page 301](#).
- Monitor-action pair – Clients connect and request channels in response to a defined monitor-action pair event. The monitor may be a schedule or another monitor type. See [“Profile – Client Actions” on page 233](#).
- Afaria-Server-initiated connection
 - Outbound notifications – Clients connect and request channels in response to the Afaria Server sending an outbound notification.
- Client API connection – Use custom applications that invoke Afaria Client APIs to initiate connections and channel requests.

Running Channels or Channel Sets on Java Clients

Afaria supports using custom application that invoke client APIs to initiate connections and channel requests.

Running Channels or Channel Sets on Handheld Clients

Afaria supports using the following options for running channels at a handheld client.

- Device- or user-initiated connection
 - Afaria Client UI – Handheld client users access the Afaria Client application on their devices to initiate a connection to the Afaria Server. Clients may be configured to request a specific channel.
 - Monitor-action pair – Clients¹ connect and request channels in response to a defined monitor-action pair event. The monitor may be a schedule or another monitor type. See [“Profile – Client Actions” on page 233](#).
- Afaria-Server-initiated connection
 - Outbound notifications – Clients connect and request channels in response to the Afaria Server sending an outbound notification.
- Client API connection – Use custom applications that invoke Afaria Client APIs to initiate connections and channel requests.

1. Monitor support on handheld clients is subject to client type. See [“Monitor Support by Client Type” on page 319](#).

Channels – Properties Tab

The Properties tab displays general properties for the item you select in the left pane's navigation tree. The page content that appears depends on the item—Server, folder, channel, or channel set—you have selected in the left pane.

Administration > Channel Administration > Properties

The screenshot displays two examples of the Properties tab. The left example, labeled "Channel > Properties", shows a "Folder" type with the name "Lost and stolen device channels" and a last updated date of 11/24/2008 11:37 AM. The right example, labeled "Folder > Properties", shows a "Patch Manager Channel" type with the name "Patch_manager_XPSP3", description "Channel created from Client Patch View", and client types "All Windows Clients". It also includes checkboxes for "Autosubscribe" and "Run only if newer", several action links (Set automatic actions..., Edit channel contents..., Examine channel contents..., View channel sets...), and a published status of "not published" with a last updated date of 12/2/2008 3:30 PM.

The Properties tab displays the following data elements:

- Type – Type of left pane selection.
- Name – User-defined name of the left pane selection. Server name is defined on the **Server configuration > Server identification** page.
- Description – Optional description of the left pane selection.
- Client type – Displays the client types associated with the channel.
- Autosubscribe – This option “forces” a subscription to occur for an Afaria Channel Viewer client or for a Windows client running a Document Manager channel parameter file (.XEC file, see “Channels – HTML Tab” on page 301). Use the attribute when you require that the client have the most up-to-date information. This option removes the Channel Viewer client’s ability to unsubscribe. Clients must first connect to the server before the autosubscribe attribute can take effect. For channels and channel sets that are associated with a schedule monitor in a group profile, the channel or channel set runs every time the schedule causes a connection, regardless of the status of the autosubscribe attribute.

If your intended behavior is to allow your Channel Viewer users to exercise discretion over whether the channel runs, then add the channel to the profile's allowed channels list, rather than associating it with a schedule.

- Run only if newer – The Run only if newer option is available only for Afaria Windows clients. It impacts only channels that run on Channel Viewer as a single channel, not those run from a Web browser or run in a channel set. This option runs the channel only if the channel's content is newer on the server than on the client.
- Published status – Displays a channel's current status, either published or unpublished.
- Last updated – Displays the time and date on which the channel was last updated, either manually or by the server schedule that updates channels.



See ["Server schedules" on page 186](#) for information about the Update Channel Contents schedule.

The Properties tab displays the following controls:

- Set automatic actions – Set date and time parameters for automatically publishing, unpublishing, and deleting the channel, and updating a channel at the server.
- Edit channel contents – Open the channel editor to edit an unpublished channel. This control is never enabled for replicated channels.
- Examine channel contents – Open a read-only view of the channel.
- View channel sets – Open a list of channel sets that includes the selected channel.



If you want to remove the channel from the set, ["Creating and Managing Channel Sets" on page 306](#).

Channels – Security Tab

The Security tab displays security attributes such as user authentication requirements or how Afaria Channel Viewer users gain access to a channel administration item. The page content that appears depends on the item—Server, folder, channel, or channel set—you have selected in the left pane.



Some security options are only available for specific client types.

Administration > Channel Administration > Security

The screenshot displays two examples of the Security tab configuration. The left example, labeled 'Channel set > Security', shows the 'Channel Viewer security' section with 'Visibility' options: 'Show in Channel Viewer' (selected), 'Hide in Channel Viewer', and 'Show during visibility window' (with a 'Set visibility window...' link). The 'Password' section has 'Required' checked and a 'Set password...' link. The right example, labeled 'Channel > Security', shows the 'Channel Viewer security' section with 'Visibility' options: 'Show in Channel Viewer' (selected), 'Hide in Channel Viewer', and 'Show during visibility window' (with a 'Set visibility window...' link). The 'Password' section has 'Required' unchecked and a 'Set password...' link. Below the 'Channel Viewer security' section, there are two checkboxes: 'Authenticate user' (unchecked) and 'Encrypt channel' (checked).

The Security tab displays the following items:

- Channel Viewer security, Visibility – Control the conditions for exposing your server-side content in the Afaria Channel Viewer application.



- Visibility is an hierarchical attribute. An item can become visible to Channel Viewer users only if any parent items are also visible. For example, a channel with the visibility attribute enabled will be visible to users only if its channel set (if any), its folder (if any), and its server are also visible.
- Document Manager channels, due to the user interaction that makes them useful, must always include channel visibility and be present in a group profile's allowed channels list to be available to Channel Viewer users.

- Show in Channel Viewer – Expose the item in Channel Viewer. This option is particularly useful when you want to distribute specific channels on a Web page.
- Hide in Channel Viewer – Do not expose the item in Channel Viewer. Use this option when you want to publish channels only on Web pages.
- Show during visibility window – Expose the item in Channel Viewer only for a specific window of time. Click **Set visibility window...** to define the date and time parameters for visibility.
- Channel Viewer security, password – Require and define a password that your Channel Viewer users must know in order to gain access to your server-side content. Click **Set password** to define and confirm a password. You must inform your Channel Viewer users of the password you set for the item.

Gaining access to an item is distinguished from being able to view an item. Use the visibility options to define whether users can view an item. Users can gain access to the item only when it is visible.

- Authenticate user – Channels only. Require the server to verify the connecting user's identity against your authentication authority before allowing the channel to run. This option is available only if you have enabled authentication on the server.



- You should enable authentication for any channels you plan to include in group profiles that have user group assignments. If you do not enable authentication, disabled domain user accounts are still able to access channels because Afaria allows the channel to run based on the user's membership in a group. Enabling authentication causes the authentication authority to evaluate the user's credentials.



- For more information about Afaria authentication, see ["Security" on page 152](#).
- Adding a channel that has the authenticate user feature enabled to a channel set makes running the entire channel set subject to the authenticate user requirements.

- Encrypt channel – Encrypt channel communications. The server uses either Microsoft Crypto API or SSL to establish secure communications, depending upon the client type.

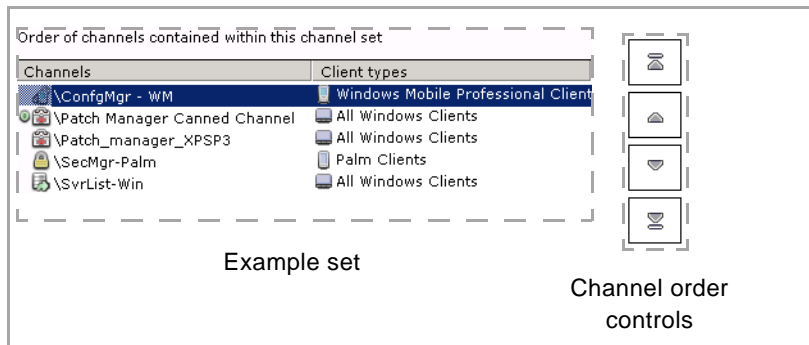


- For more information about Afaria encryption, see ["Client communication" on page 119](#).

Channels – Channels Tab

The Channels tab displays the channels that belong to a channel set. The list is sorted in order of execution; the top channel executes first. Use the page to change the order of execution and to add channels to or remove channels from the set.

Administration > Channel Administration > Channel set > Channels



The set list includes the following information:

- Channels – Channel administration tree path to the channel and the user-defined channel name.
- Client types – The client types selected for the channel.

Sets can contain channels for a mixed variety of clients types and channels in any publication state, published or unpublished. Changing a member channel's publication state lets you effectively enable or disable the channel within the set without changing the set's membership.

To change the order of a channel in the channel set:

- 1 Select a channel on the set list.
- 2 Click an order control to change a channel's execution order in the set.
- 3 Save your changes.

To add or remove channel set channels:

- 1 Select a channel set in the left pane.
- 2 Select the **Channels** tab in the right pane.
- 3 Click **Add/Remove channels...** at the bottom of the right pane to open the channel selection dialog box. The box contains a channel tree similar to the tree in the left pane.
- 4 Select or clear the check boxes next to the channels to add or remove channels. Selecting a folder or channel set adds the channels included in that item to your current set, not the folder or channel set itself.

5 Save your changes.

Channels – Profiles Tab

The Profiles tab displays the profile membership for a channel or channel set. The page is informational only; use the group profile user interface or the new channel wizard to assign or remove channels or channel sets.

Administration > Channel Administration > Channel or Channel set > Profiles

Profile	Description
Building 1245 secure access SW Sales	Building 1245 employees that SW Sales Reps and Managers

The set list includes the following information:

- Profile – User-defined profile name from the group profile user interface.
- Description – The optional description for the profile.

Channels – HTML Tab

Supported client types – Windows, Windows Mobile Professional, Windows Mobile Standard

Use the HTML tab to create a channel parameter file. A parameter file contains all the information a client needs to initiate a connection and request a channel. A client can execute a parameter file from a Web page, from a network or local file storage location, or via some other delivery method such as an e-mail.

The Afaria Server generates the HTML code appropriate for publishing the parameter file on a Web page. The HTML code references the parameter file and the control type you choose to launch the channel; an image, text, or other control.



Server Listing channels are not eligible for parameter-file-based publication.

Administration > Channel Administration > HTML

Generate HTML parameter file
Control type:
Text:
Parameter file:

```
<!-- Afaria HTML Template: Text
NOTE: You must save the parameter file to the
directory in which you place your HTML
file.-->
<p>
<a href="Patch_Manager_Canned_Channel.xec">Enter button label or anchor text here</a>
</p>
```

Show all status
 Hide messages [Copy to clipboard](#)
 Disable messages [Test HTML](#)
 Hide all status

 Close UI immediately

The HTML tab contains the following fields and options:

- Generate HTML parameter file – This option enables both creating the channel parameter file and exposing the supporting HTML code for publishing the parameter file on a Web page. Parameter files are created with an XEC extension.
- Control Type – For Web-based publication, this option lets you select the type of control you want to use on the Web page to access the channel. Depending on the control type you select, one of the following fields appears:
 - Text – The channel appears as a hyperlink. When you select this option, you are prompted to type anchor text in the **Text** field.

- Button text – The channel appears as a standard button on a Web page. When you select this option, you are prompted to type a button label in the **Button text** field.
- Image – The channel appears as a jpeg or gif image on the Web page. You can type the file name in the **Image** field or click **Browse...** to navigate to the appropriate file.

The HTML code defaults to referencing the image file in the same folder as where the HTML executes. You may store the image file and the HTML code in separate folders as long as you update the HTML code to reference the alternate image file location.

- Connect on load. When you select this option, the channel runs immediately when the Web page displays. No channel-related item (button, text, etc.) appears on the Web page itself.



When you select the Connect on load option, you must change the URL to include a Web server and the correct path for the parameter file.

- Parameter file – This field displays the path to the parameter file. You can click **Browse...** to change the location of the file. If you use an image as the control type, you must place the file into the same directory as well.



- The HTML code defaults to referencing the parameter file in the same folder as where the HTML executes. You may store the parameter file and the HTML code in separate folders as long as you update the HTML code to reference the alternate parameter file location.
- If the parameter file is deleted from the system for any reason, you will have to make some change to the channel in order to re-enable the Save option.

- Show all status – This option enables a client window to open when the session runs with status messages visible to the user.
- Hide messages – This option enables a client window to open when the session runs with status messages hidden from the user. The window exposes a **Messages** button the user can choose to expose or hide the status messages.
- Disable messages – This option enables a client window to open when the session runs, but with status messages hidden from the user and without the capability to expose status messages.
- Hide all status – This option does not open any client window when the session runs.
- Close UI immediately – This option automatically closes the client window when the session is complete. This does not close the client user's Web browser.
- Copy to clipboard – You can select this option to transfer the HTML code to the Windows clipboard so that you can paste it into any other application.

- Test HTML – You select this option to test the control you selected for running the Web page. Your Web browser opens, and the control appears. Click the control to test the channel.
-



- Although you can publish a Document Manager channel on a Web page, the browser does not display controls for subscribing to a document. Therefore, users are unable to select documents for subscription. Consider using the autosubscribe attribute on the Properties page, which subscribes users and keeps documents current without requiring user interaction.
- To publish channels for clients running a Web browser other than Microsoft Internet Explorer, you must manually register the Afaria MIME type on your Web server. See your Web server documentation for information on how to register MIME types for your specific server. You will need to register the Afaria XEC file extension to “application/x-Xessentials”.

Creating a Channel

Create a channel to define work for a client. When you create channel, they appear in a tree directory beneath the server in the left pane of the window. By default, channels appear in the order of a system-defined sort, but you can create folders to contain collections of channels.

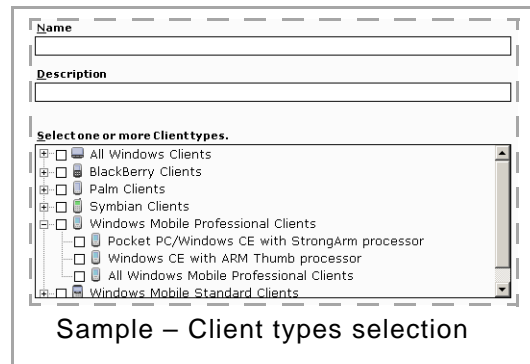
Administration > Channel Administration > New... Channel type

This topic describes creating a channel from the Channels Administration page. However, you can also create a new channel from the group profile UI.



- 1 Click **New... > Channel type...** to open the channel wizard's Client types dialog box.

The Client types dialog box appears. The channel type referenced in the window's title bar varies depending on the channel you are creating.



- 2 Type a unique **Name** for the channel and an optional **Description**.

- 3 Select the check box next to the **Client type** you want to associate with this channel.

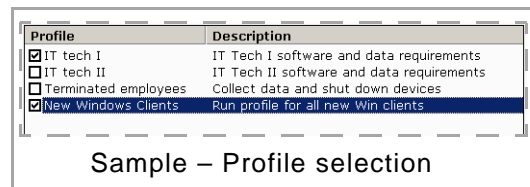
Only the client types available for that channel type that you have licensed appear in the list. Not all channel features apply to all client types.



With the exception of Session Manager channels, Afaria channels are dedicated to a single client type at a time. For example, if you want to create a Document Manager channel for both Windows and Palm client users, you must create two separate channels.

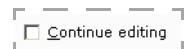
- 4 Click **Next** to open the Profile selection page dialog box. This dialog box displays any profiles that match the channel's client type. You can select any profiles in the list.

Selecting a profile will add the current channel to the profile's list of allowed channels. See ["Profiles" on page 222](#).



- 5 Click **Next** to continue to the next wizard page. Some channel types have additional wizard pages to prompt for channel-type-specific requirements. See *Afaria Reference Manual | Components*.

The final wizard page may include a check box you can select to automatically open the channel editor for further editing.



Channels and channel sets have behaviors that are best understood in a shared context. Learn more about the following properties that apply to channels and channel sets:

- ["Channels – Properties Tab" on page 294](#)

- [“Channels – Security Tab” on page 296](#)
- [“Channels – Channels Tab” on page 298](#)
- [“Channels – Profiles Tab” on page 300](#)
- [“Channels – HTML Tab” on page 301](#)

Creating and Managing Channel Sets

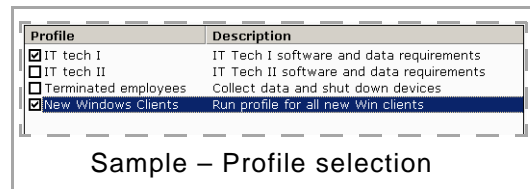
Create channel sets to execute multiple channels together.

This topic describes creating a channel set from the Channels Administration page. However, you can also create a new channel set from the group profile UI.



- 1 Click **New... > Channel set...** to open the New channel set dialog box.
- 2 Type a unique **Name** for the channel and an optional **Description**.
- 3 Choose **OK** to continue to the profile selection page. This page displays existing profiles. You can select any profile in the list.

Selecting a profile will add the current channel set to the profile's list of allowed channels. See ["Profiles" on page 222](#).



- 4 Choose **Next** to continue to the wizard's channel selection page. Select channels from the channel navigation tree.
- 5 Choose **Next** to continue to the channel order page. Channels run in order of top to bottom. Select a channel and click the order controls to move channels up or down the list of channels.
- 6 Choose **Finish** to complete the wizard. The channel set appears on the Channels Administration page in the left pane.

Once you have created a channel set, you can use the controls on the Channels tab to add or remove channels and to reorder individual channels within the set.

Channels and channel sets have behaviors that are best understood in a shared context. Learn more about the following properties that apply to channels and channel sets:

- ["Channels – Properties Tab" on page 294](#)
- ["Channels – Security Tab" on page 296](#)
- ["Channels – Channels Tab" on page 298](#)
- ["Channels – Profiles Tab" on page 300](#)
- ["Channels – HTML Tab" on page 301](#)

Publishing a Channel



Publish channels to make them available for client users via their group profiles. To publish a channel, you can select it in the left pane and click the **Publish** icon on the toolbar, or you can select **Publish** on the channel's shortcut menu. A green dot icon appears next to the channel in the left pane to indicate that it has been published.



To unpublish a channel, you can select it in the left pane and click the **Unpublish** icon on the toolbar, or you can select **Unpublish** on the channel's shortcut menu.



Publishing a working copy will overwrite the original channel and publish it, even if the original was unpublished. Unpublishing a channel will not interrupt service to currently connected clients. However, the channel will not be available to clients connecting after the channel is unpublished.

See [“Group Profiles and Channels” on page 290](#) for detailed information about making channels available for client users.

Editing a Channel

Edit a channel when you want to change some of a channel's properties. You can edit unpublished channels or published channels. In the case of published channels, except Session Manager channels, you can edit the channel by first making a working copy, and then editing the working copy. Once you have made the necessary changes to the working copy, you can publish the edited channel. The new channel takes the place of the original.



Editing Session Manager channel contents – The worklists and sendlists that you create and edit in the Session Manager Channel Editor are objects independent from the Session Manager channel. You can assign these objects to multiple Session Manager channels. Because these objects are independent, any changes you make to an object in one channel affect all other channels assigned to that object.



Working copies of channels display a pencil to the left of the channel icon and also have a (w) at the end of the channel's name.

To edit a channel or a working copy of a channel, select it in the left pane and click **Edit channel contents**. The channel-specific editor opens so you can edit the channel.



- You can also use the Cut, Copy, and Paste icons on the toolbar to move folders and channels from one location to another.
- Copying a channel does not preserve the channel's automatic actions and HTML settings.

Copying a Channel

Copy a channel to create a new, independent channel.



- 1 Right-click the channel to copy and select **Copy**.
- 2 Right-click the target node in the channel tree, such as the server or folder, and select **Paste**.

Considerations for Copying a Channel

The results for copying channels differ according to several factors, including the type of channel and its properties.

Consider the following items when copying channels:

- Channel names – The system renames the channel to something unique in the target location.

A channel name, in this context, is evaluated as its folder path plus the channel name. For example, a channel named “Hardware” stored in nested folders “Inventory\Windows” is evaluated as “Inventory\Windows\Hardware.” Copying channel “Inventory\All\Hardware” into folder “Inventory\Windows” results in the system renaming the channel during the copy to prevent a conflict with the other “Hardware” channel.
- Channel HTML properties – Channels do not retain their HTML properties during a copy action.
- Session Manager:
 - Worklists – The system copies pointers to the worklists but does not copy the worklists.
 - (Multitenancy) Shared worklists – The system copies pointers to the worklists but does not copy the worklists.
 - (Multitenancy) Tenant-specific worklists – The system copies the worklist with any paths and pointers to other channels but does not copy any referenced channels. For example, it copies a worklist’s Insert event that references a channel to insert, but does not make a copy of the referenced channel.
- Software Manager, Document Manager – The system copies the paths and pointers to channel delivery objects but does not copy the objects. For example, it copies the Document Manager channel defined path to a document but does not make a copy of the document itself.

About Importing and Exporting Channels

You can import and export channels from one server to another server that are not in a server farm relationship with each other. Exported channels are independent from their source server. After exported channels are imported into another server, they are subject to any editing tasks the administrator wants to exercise. This differs from replication, in that replicated channels are read-only channels that you can edit only at the source server.

The product includes an import/export wizard, to import and export using the user interface, and a command line utility, to import and export from a command line.

Considerations for Importing and Exporting Channels

The results for importing and exporting channels differ according to several factors, including the type of channel and its properties.

Consider the following items when importing and exporting channels:

- Duplicate channel names – You cannot import a channel with a name that already exists in the importing environment unless you indicate replace (import wizard) or overwrite (utility command line) in the import definition.

A channel name, in this context, is evaluated as its folder path plus the channel name. For example, a channel named “Hardware” stored in nested folders “Inventory\Windows” is evaluated as “Inventory\Windows\Hardware.” Copying channel “Inventory\All\Hardware” into folder “Inventory\Windows” results in the system renaming the channel during the copy to prevent a conflict with the other “Hardware” channel.

- Channels with user authentication – If you import a channel that has authentication enabled, and you do not have authentication enabled on your server, any client that tries to connect to the channel receives an “authentication failed” message. Enable authentication on the Security page in Server configuration, Properties.
- (Multitenancy) Tenant associations:
 - Imported channels, wizard import – Imported channels associate with the importing tenant.
 - Imported channels, utility import – Imported channels associate with the tenant parameter you specify. If you omit a tenant parameter, the channel imports into the tenant that exported the channels, as identified in the export file. If you specify multiple tenants, the last tenant is the importing tenant.
 - Exported channels, utility export – Exported channels associate with the tenant parameter you specify. If you specify multiple tenants, the first tenant is the exporting tenant.
- Software Manager, Document Manager – The system export behavior relating to channel delivery objects, such as documents for Document Manager channels, is defined when executing the export. The import process imports what is included in the exported file.
- Session Manager – Consider the following items about Session Manager channels:
 - (Nonmultitenancy) Worklists – Worklists always overwrite worklists by the same name, regardless of the setting of the replace/overwrite attribute.

- (Multitenancy) Shared worklists – The imported worklist associates with the system tenant. If the system tenant already has the worklist, it is preserved and the imported channel is modified to point to it.
- (Multitenancy) Tenant-specific worklists – The imported worklist associates with the importing tenant. If another tenant already has the worklist, the import fails.
- Channel sets – Importing or exporting a channel set does not also imply the action for its associated channels. Explicitly select channels for import or export.

Importing a Channel

Afaria uses an import wizard to guide you through the following import steps.



To import a channel, you select the **Import/Export** icon on the toolbar. The channel import and export dialog box appears. Select **Import**.

Selecting the Import File

Use this step to enter the path and name of the file to import, or click **Browse...** to navigate to the file. The extension for channel files is CMX.

Selecting Items to Import

Use this step to select the channels you want to import to your server.

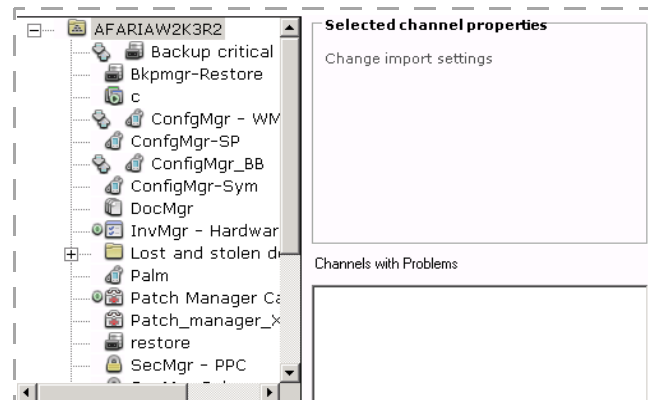


Importing a channel with the same name as an existing channel will automatically overwrite the existing channel.

In the Select channel to import area, you can select the check box next to each channel you want to import, or you can click **Select Branch** to select all of the channels listed.

In the Select target location area, you select the server where you want to import the channels. What you do next depends on the type of channel you want to import:

- To import a new channel, select the source channel on the left and select the target server or folder on the right and click **Add**. The channel appears in the list the Import/Export icon next to it.



- To import an updated version of a channel that already exists on the target server, select the source channel on the left and select the target channel on the right and click **Replace**. The channel appears in the list with the Import/Export icon next to it.
(Multitenancy) Replace is not a valid action when using the system tenant context.
- To remove a channel you do not want to import, you select it in the target location list box and click **Remove**.

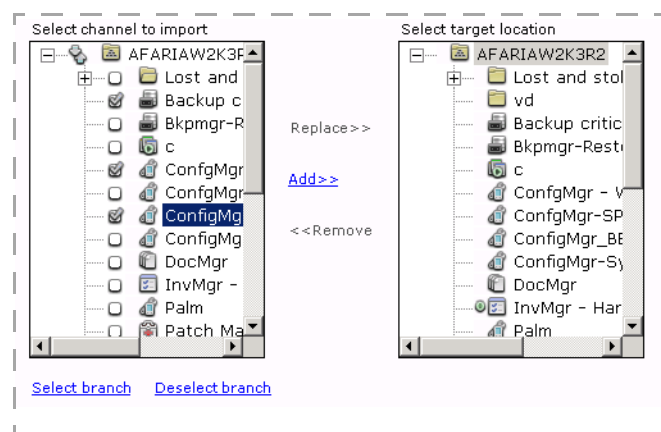
Defining Import Settings

Use this step to verify that the channel is ready to be imported, or to change import settings for a channel.

First, you should verify that the channel you are importing has the Import/Export icon next to it. This indicates the channel is ready to import. For some channels, you can click **Change import settings** to change the settings for this channel and repeat this step until the Import/Export icon appears, verifying the channel is ready to import.

If a channel cannot be imported, it appears in the Channels with problems list box. For example, if you are trying to import a LAN-based Software Manager channel that associates with files from a shared point on the network that is no longer available, the channel is invalid because it can no longer access those files.

Click **Finish** to complete the wizard. The imported channels appears on the specified server.



Exporting a Channel

Afaria uses an export wizard to guide you through the following export steps.



To export a channel, you select the **Import/Export** icon on the toolbar. The channel import and export dialog box appears. Select **Export**.

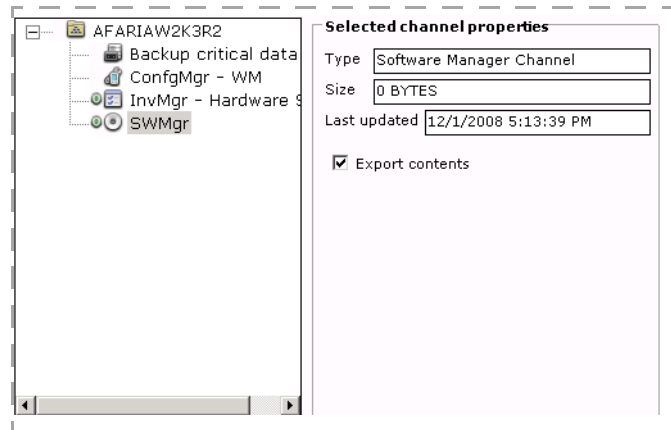
Selecting Items to Export

Use this step to select the items you want to export from a selected server by selecting the check box next to the items.

Defining Export Settings

Use this step to determine which channel settings to export with the channel. You may choose to export only the channel itself, or all of the contents, properties, and security settings that make up the channel.

Select each channel in your export list to review the selected channel properties that display on the dialog box. If the channel is not a Session Manager channel and has external files associated with it, such as a Document Manager channel, then the **Export contents** check box becomes enabled. Exporting contents exports the associated files along with the channel definition.



You may prefer to not export the contents if the planned importing server has access to the files using the same relative path as the exporting server.

When you click **Next** to continue, the Select export file dialog box appears.

Selecting the Export File

Use this step to enter the path and name of the file to store the channel export, or click **Browse...** to navigate to the file. The extension for channel files is CMX.

Import/Export Channel Utilities

Afaria includes command-line utilities to execute channel import and export commands.

Command path: <ServerInstallDir>\bin\

Command for import: xaimport

Command for import help: xaimport /?

Command for export: xaexport

Command for export help: xaexport /?

The same considerations that apply to using the UI to execute the commands apply to using the utility.

See also, [“Importing a Channel” on page 311](#) and [“Exporting a Channel” on page 312](#) to review the considerations.

About Outbound Notifications



Before sending notifications, see [“Managing Client Outbound Notification Addresses” on page 416](#) for information on establishing connection addresses.

An outbound notification is a set of instructions that is sent from an Afaria Server to an Afaria Client. The instructions tell the client to initiate a connection back to its server to request a specific channel.


The outbound notification feature requires that a “listener” is present at the client. The server delivers the listener to the client during the client’s first connection. Therefore, a client must have had at least one successful Afaria connection before the server can send, and the client can receive, an outbound notification.



Afaria includes a public Web service for the outbound notification feature so that you can offer the service without requiring access to your Afaria Administrator server. Contact your Afaria account representative for more information.

Sending an Outbound Notification

Initiate an outbound notification to a client when you want the client to connect to an Afaria Server right away to request a specific channel. To run, the channel must be included in one of the client's group profile allowed channels list. See ["Profile – Allowed Channels" on page 240](#) to learn more about the allowed channels list.

- 1 On the Channels Administration page, select a published channel or channel set. The channel or channel set you select must be associated with a client type that supports outbound notifications.
- 2  Choose **Outbound notification** on the toolbar. The resulting submenu's options are based on whether there are assignments associated with the channel.
 - **Clients...** – When you select this option, the Outbound notification dialog box opens and includes all client types that support outbound notifications. You can select one or more clients for notifications.
 - **Assigned Client groups...** – When you select this option, the Outbound notification dialog box opens and includes all the client groups currently assigned to all of the profiles associated with the channel. Select the check box next to a client group to initiate a notification with all group members.



You cannot select clients based on user group membership.

- 3 Choose **OK** to send the notification.

The Sending Client Notification dialog opens after you send an outbound notification to display Afaria Server send status and to display notifications sent status. See ["Client Notifications Status" on page 419](#) for dialog details.

If notification was successful, the client attempts to connect to the server and request the selected channel. The Messages log captures the success or failure of sending the outbound notification. The Sessions log captures the success or failure of the requested channel.

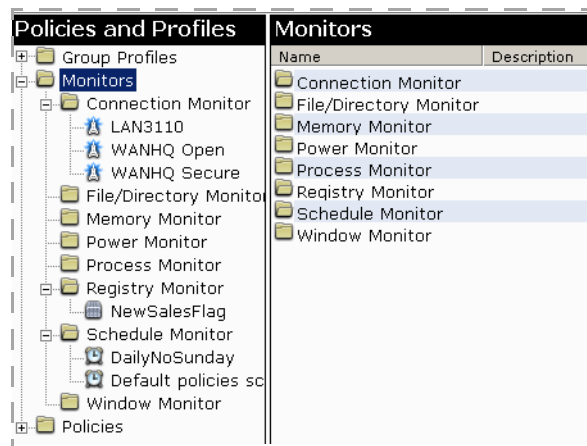
Monitors

Supported client types – Afaria clients

Use the Monitors area of the Afaria Administrator to define and manage device monitors. Device monitors enable you to detect or schedule events on clients. For example, you can create a schedule monitor to detect when the last Friday of the month occurs, and then take some type of predefined action. Deploy monitors to clients as part of a group profile. When the monitored condition or event occurs, the predefined action is taken automatically.

In a server farm environment, you can view monitors from any server. However, you must be on the main server to create or edit monitors.

Administration > Policies and Profiles



About Monitors

Device monitors allow you to monitor the client for specific activity or data items according to criteria that you define. Monitors are composed of the following elements:

- Name and description – user defined
- Monitor attributes – Pre-defined type selection
- Hours of operation – Flexible time and day definition

Group Profiles and Monitors

Profiles are the vehicles for distributing monitors to client devices; monitors are components in the profile's definition. Include monitors with profiles via a profile's Client Actions list in order to associate them with Afaria clients. When a monitor is associated with an action in a profile, it is called a monitor-action pair. See ["About Profiles" on page 223](#) for more information.

Monitor Types

The following monitor types are available:

- Connection monitor – Detects when a network connection becomes active, i.e., connected. The monitor can watch for any network connection or a specific connection name.
- File/Directory monitor – Monitors the creation or deletion of new files or new directories. Directories may be monitored for any changes.
- Memory monitor – Monitors available memory levels.
- Power monitor – Monitors the status of the power source and/or battery levels.
- Process monitor – Monitors the launch of executable files.
- Registry monitor – Checks the registry for the creation, change or deletion of a specific value under a registry key.
- Schedule monitor – Waits for a time of day, day of the week, day of the month, or a one-time scheduled event. Most schedule monitors can operate with recurrence.
- Window monitor – Monitors the creation or destruction of a specified window.



New monitors are delivered via the channel listing. The channel listing is delivered when an Afaria Client connects to the Afaria Server and the client is assigned to the profile or is a member of a group assigned to the profile.

Create additional monitors using the monitor wizards associated with each monitor type.

Administration > Policies and Profiles > New > Monitors > *monitor type*

Select the time and date to run the schedule.

Start time

Of the following day(s)

Day(s) of the month [Select day\(s\) ...](#)

The

Of the following month(s)

<input checked="" type="checkbox"/> January	<input checked="" type="checkbox"/> April	<input checked="" type="checkbox"/> July	<input checked="" type="checkbox"/> October
<input checked="" type="checkbox"/> February	<input checked="" type="checkbox"/> May	<input checked="" type="checkbox"/> August	<input checked="" type="checkbox"/> November
<input checked="" type="checkbox"/> March	<input checked="" type="checkbox"/> June	<input checked="" type="checkbox"/> September	<input checked="" type="checkbox"/> December

Run at startup if schedule was missed

Randomize start time by

Monthly Schedule Monitor wizard sample

Indicate the power settings you want to monitor.

Events

Change to battery power

Change to external power

Low battery level

Threshold %

Reset threshold %

Polling interval Units

Power Monitor wizard sample

Monitor Support by Client Type

Although device monitors are not device-specific, feature availability depends on client type features and platform support. For this reason, device monitors may function differently between client types. See the following table to learn about monitor support by client type.

<i>Client type^a:</i>	<i>Windows Mobile^b</i>	<i>Windows CE^c</i>	<i>Windows</i>	<i>Symbian</i>	<i>BlackBerry</i>
Connection	X	X	X		
File/Directory	X				
Memory	X				
Power	X				
Process	X				
Registry	X				
Schedule	X	X	X	X	X
Window	X				

a. Palm and Java devices do not support monitors.

b. Includes Windows Mobile Professional and Windows Mobile Standard.

c. A subtype of Windows Mobile Professional.

Monitor Substitution Variables

Some monitors support the use of substitution variables. The variables provide access to event-related, monitor data when using other components of Afaria. Substitution variables can be used or accessed in:

- Afaria logs – See [“Working with Logged Actions” on page 439](#).
- A Session Manager channel initiated by a profile’s monitor-action pair – The substitution variables are private, session variables when used in the Session Manager Channel Editor. You must enter monitor variables manually, i.e., they are not available from the editor’s Session Variables list. See *Afaria Reference Manual | Components*, Session Manager for additional information about using variables in a Session Manager channel.
- An Execute Program action or Run Script action initiated by a profile’s monitor-action pair – You can pass the substitution variables as Parameters in the Action Editor. See [“Defining the “Execute Program” Action” on page 236](#) and [“Defining the “Run Script” Action” on page 237](#).

To use the variables in the Session Manager Channel Editor or the Action Editor, enter the full variable name enclosed by angle brackets. For example, `<MonitorData1>`.

Exporting and Importing a Monitor

Export and import features are available as part of the profile export and import feature. See [“Importing a Profile” on page 226](#) and [“Exporting a Profile” on page 227](#).

Creating a Monitor

You can create a monitor from the **Administration > Policies and Profiles** area, or when using group profiles. See [“Profile – Client Actions” on page 233](#) to learn more.

- 1 Begin on the Administration, Monitors page.
- 2 Click **New > Monitors > monitor type** on the toolbar to open the wizard for that monitor.
- 3 Type a **Name** and optional **Description** for the monitor.
- 4 Click **Next** to continue. The wizard provides a set of monitor settings depending on the type of monitor selected. See the following topics for monitor setting details.
 - [“Connection Monitor Settings” on page 325](#)
 - [“File/Directory Monitor Settings” on page 327](#)
 - [“Memory Monitor Settings” on page 329](#)
 - [“Power Monitor Settings” on page 331](#)
 - [“Process Monitor Settings” on page 332](#)
 - [“Registry Monitor Settings” on page 335](#)
 - [“Schedule Monitor Settings” on page 337](#)
 - [“Window Monitor Settings” on page 344](#)
- 5 After completing the monitor settings for your monitor type, click **Next**. If supported by the monitor type you are creating, the hours of operation settings display.



-
- By default, the **Enable hours of operation** check box is cleared, indicating that the monitor will run continuously.
 - See [“About Hours of Operation” on page 323](#) for examples of hours of operation functionality.

- **Enable hours of operation** – Select this box to enable the settings for defining the time when the monitor is active.
 - **Start time** – Select a start time to begin the monitor.
 - **End time** – Select an end time to stop the monitor.
 - **On the following day(s)** – Specify the days when the monitor is active.
- 6 Click **Finish** to complete the wizard.

Editing a Monitor

Edit a monitor to make changes to an existing monitor's defined settings or hours of operation definitions. You can edit monitors even if you have already associated the monitor with one or more group profiles. Afaria deploys the updated monitor to assigned clients during their next Afaria sessions. See ["About Profiles" on page 223](#).

To edit a monitor, double-click it in the **Monitors** column. The system displays an editor dialog box for the monitor selected. You can also edit a Monitor when using profiles. See ["Profile – Client Actions" on page 233](#).

See the following topics for monitor setting details:

- ["Connection Monitor Settings" on page 325](#)
- ["File/Directory Monitor Settings" on page 327](#)
- ["Memory Monitor Settings" on page 329](#)
- ["Power Monitor Settings" on page 331](#)
- ["Process Monitor Settings" on page 332](#)
- ["Registry Monitor Settings" on page 335](#)
- ["Schedule Monitor Settings" on page 337](#)
- ["Window Monitor Settings" on page 344](#)

About Hours of Operation

When working with the hours of operation settings, there are three major variations to consider:

- Start time is set earlier than the end time.
- Start time is later than the end time
- Start time and end time are the same

File/Directory Monitor Wizard - Hours of operation

Indicate the hours and days of the week you want this monitor to function.

Enable hours of operation

Start time: 9:00:00 AM End time: 5:00:00 PM

On the following day(s)

<input type="checkbox"/> Sunday	<input checked="" type="checkbox"/> Thursday
<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Friday
<input checked="" type="checkbox"/> Tuesday	<input type="checkbox"/> Saturday
<input checked="" type="checkbox"/> Wednesday	

For hours of operation extending into the next day, only select the day monitoring is to begin.

<Back Finish Cancel

If the start time is earlier than the end time, the monitor will start and stop at the times specified for each day selected. In this example, the monitor starts at 9:00 a.m. and stops at 5:00 p.m. Monday through Friday.

File/Directory Monitor Wizard - Hours of operation

Indicate the hours and days of the week you want this monitor to function.

Enable hours of operation

Start time: 5:00:00 PM End time: 10:00:00 AM

On the following day(s)

<input type="checkbox"/> Sunday	<input type="checkbox"/> Thursday
<input type="checkbox"/> Monday	<input type="checkbox"/> Friday
<input checked="" type="checkbox"/> Tuesday	<input type="checkbox"/> Saturday
<input type="checkbox"/> Wednesday	

For hours of operation extending into the next day, only select the day monitoring is to begin.

<Back Finish Cancel

If the start time is later than the end time, the monitor will start for the day selected, and will not stop until the specified time on the following day. In this example, the monitor will start at 5:00 p.m. on Tuesday and run continually until it stops at 10:00 a.m. on Wednesday.

File/Directory Monitor Wizard - Hours of operation

Indicate the hours and days of the week you want this monitor to function.

Enable hours of operation

Start time: 10:00:00 AM End time: 5:00:00 PM

On the following day(s)

<input type="checkbox"/> Sunday	<input type="checkbox"/> Thursday
<input checked="" type="checkbox"/> Monday	<input type="checkbox"/> Friday
<input checked="" type="checkbox"/> Tuesday	<input type="checkbox"/> Saturday
<input checked="" type="checkbox"/> Wednesday	

For hours of operation extending into the next day, only select the day monitoring is to begin.

<Back Finish Cancel

If the start time and end time are the same, the monitor will run for the entire day and not stop until the specified time on the day specified. In this example, the monitor will start on Monday at 10:00 a.m., run all day Tuesday, and stop on Wednesday at 10:00 a.m.

Common Monitor Settings

Administration > Policies and Profiles > New > Monitors > *monitor type*

Some properties are common to most monitors, as noted in the table below. An “X” indicates a monitor uses the common property. A blank indicates a monitor does not use the property.

	<i>Common property:</i>	<i>Blackout interval</i>	<i>Polling interval^a</i>
Connection		X	X
File/Directory		X	
Memory			X
Power			X
Process		X	X
Registry			
Schedule			
Window		X	X

a. For Windows Mobile 5 or later devices, the monitors do not use the polling interval.

Blackout interval – Defines a period, after having detected a monitored event, during which a monitor will not report additional activity. If the blackout interval expires while a monitored condition is active, the monitor will not register the condition until it occurs again. Use of the interval prevents multiple events from being detected within the period you define.

Polling interval – Specifies how often the monitor will check the client for the condition you define. Shorter polling intervals produce the most accurate results, but also contribute to an accelerated decrease in battery life.



If you deploy monitors of the same type to poll a client device, the smallest defined polling interval is always used for that monitor type.

Connection Monitor Settings

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

The Connection monitor watches for the activation of a network connection on the client. The monitor can watch for the activation of any available network connection, or a connection of a specific name.

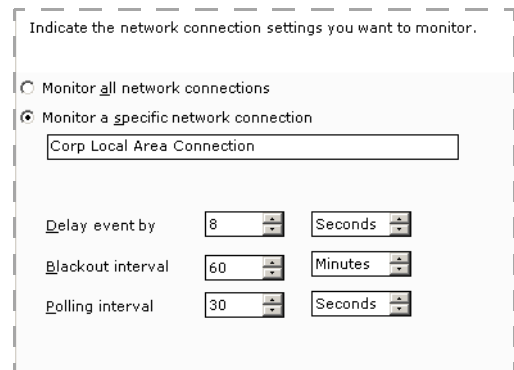
The monitor detects network connection status changes. When the status of the connection changes from an inactive state to an active state, i.e., connected, the monitor registers the change.

Administration > Policies and Profiles > New > Connection Monitor > Settings

- **Monitor all network connections** – Detects the activation of any network connection on the client.
- **Monitor a specific network connection** – Detects the activation of a specific network connection on the client. When selected, provide the network connection name as defined on the client.

Afaria can monitor a specific GPRS network connection only if the device uses Remote Access Services (RAS) to manage the connection.

- **Delay event by** – Provides an interval, if required, for the client device to complete the network connection prior to the monitor registering connection availability.



Indicate the network connection settings you want to monitor.

Monitor all network connections

Monitor a specific network connection

Corp Local Area Connection

Delay event by 8 Seconds

Blackout interval 60 Minutes

Polling interval 30 Seconds

Detecting a Connection by Client Type

The transition of a network connection from an inactive state to an active state is detected differently among supported client types:

- Windows Mobile 5 and later – Polling is not used to detect a change in connections.
- Windows CE (Windows Mobile Professional subtype) – The monitor detects a watched connection only after a successful socket connection with an Afaria Server occurs.
- Windows – Monitor polling detects an active, watched connection only after it is opened.

Substitution Variables

The following substitution variables are available when using the Connection monitor:

- <MonitorData1> – Contains either “Any Connection” or “Specific Connection”, depending on how you’ve configured the monitor.
- <MonitorData2> – Provides a specific connection name if you’ve configured the monitor to watch for a specific connection. If you’ve configured the monitor to watch any connection, contains an empty string.
- <MonitorData3>, <MonitorData4>, <MonitorData5> – Reserved for future use.

See [“Monitor Substitution Variables” on page 319](#) to learn more.

Deployment and Usage Considerations

Consider the following when using Connection monitors:

- The connection monitor captures state changes, therefore a network connection that is active at the time of deployment to a client is not detected by the monitor.
- When a wireless connection is defined as a device’s default configuration—that is, the device’s settings without regard to the Afaria Client configuration settings—and the device goes into suspend mode, the radio may become disabled. If the radio becomes disabled, Afaria may be unable to initiate a wireless connection and the user may receive a message that the connection and the session failed.
- Windows Mobile 2003—A device that transitions into suspend mode may delay the polling interval.

File/Directory Monitor Settings

Supported client types – Windows Mobile Professional (excluding Windows CE), Windows Mobile Standard

Use the File/Directory monitor settings to watch for the creation of new files or directories and changes to existing files or directories. Substitution variables may be used when specifying the file or directory client path name. Allowed substitution variables are:

- <Favorites> – browser favorites
- <Fonts> – virtual folder for fonts
- <Personal> – repository for the “\my documents” folder on most Windows Mobile 5 and later devices
- <Programs> – directory containing user’s program groups
- <StartMenu> – directory containing Start menu items
- <Startup> – directory corresponding to user’s Startup
- <MyMusic> – directory containing user’s music files
- <Windows> – the Windows folder
- <ProgramFiles> – the Program Files folder

These variables must be used as the first component of the path name. See [“Monitor Substitution Variables” on page 319](#) to learn more.



You cannot monitor the root directory of a Windows Mobile Professional device.

Administration > Policies and Profiles > New > File/Directory Monitor > File settings

Client path name. Type a valid path name for the file to monitor.

Events. Select an event or events in any combination:

- File created – detects a new file.
- File deleted – detects a file deletion.
- File modified – detects for file changes.

The screenshot shows a dialog box with the following elements:

- Two radio buttons: File and Directory.
- A text input field labeled "Client path name".
- An "Events" section containing three checkboxes: File created, File deleted, and File modified.

Administration > Policies and Profiles > New > File/Directory Monitor > Directory settings

Client path name. Type a valid path name for the directory being monitored.

Events. Select an event or events in any combination:

- Directory created – detects a new directory.
- Directory deleted – detects a directory deletion.
- Directory contents changes – detects directory changes only at the root level.
- Include sub-directories – extends the detection changes to sub-directories for the specified directory.

Indicate the file/directory settings you want to monitor.

File
 Directory

Client path name

Events

File created
 File deleted
 File modified

Blackout interval Units

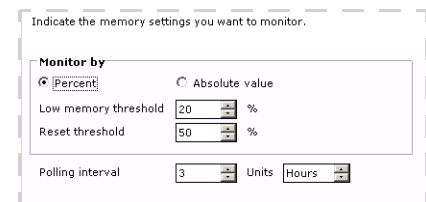
Memory Monitor Settings

Supported client types – Windows Mobile Professional (excluding Windows CE), Windows Mobile Standard

Use the Memory monitor settings to watch for specifically-defined available memory and low memory thresholds based on either the percentage of free memory or when memory levels fall below a defined parameter. The memory monitor allows an administrator to see patterns of memory usage on a client in order to optimize productivity and work efficiency. You can set the memory monitor by percent or absolute value.

Administration > Policies and Profiles > New > Memory Monitor > Percent settings

- **Low memory threshold** – Defines the lowest percentage of memory that can be reached before an event is triggered.
- **Reset threshold** – Defines the percentage of memory that must be achieved before the low monitor threshold triggers another event. If the percentage of memory remains below the low memory threshold, the monitor will not be triggered.



Indicate the memory settings you want to monitor.

Monitor by

Percent Absolute value

Low memory threshold %

Reset threshold %

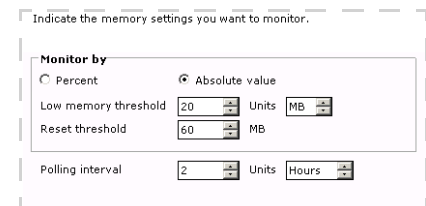
Polling interval Units



Reset threshold values for percent and absolute values must be greater than the low memory thresholds you define.

Administration > Policies and Profiles > New > Memory Monitor > Absolute value settings

- **Low monitor threshold** – Defines the lowest specific memory value that can be reached before an event is triggered.
- **Reset threshold** – Defines the specific memory value that must be achieved before the low monitor threshold triggers another event. If the specific memory value remains below the low monitor threshold, the monitor will not be triggered.



Indicate the memory settings you want to monitor.

Monitor by

Percent Absolute value

Low memory threshold Units

Reset threshold MB

Polling interval Units



Reset thresholds values for percent and absolute values must be greater than the low memory thresholds you define.

Substitution Variables

The following substitution variables are available when using the Memory monitor:

- <MonitorData1> – Contains the absolute value of free memory that caused the monitor to fire.
- <MonitorData2> – Contains the percentage of free memory that caused the monitor to fire.
- <MonitorData3>, <MonitorData4>, <MonitorData5> – Reserved for future use.

See [“Monitor Substitution Variables” on page 319](#) to learn more.

Power Monitor Settings

Supported client types – Windows Mobile Professional (excluding Windows CE), Windows Mobile Standard

Use the Power monitor settings to define events that watch for changes in power sources, and to indicate battery levels at defined thresholds. The settings can be selected in any combination.

Administration > Policies and Profiles > New > Power Monitor > Power settings

- **Change to battery power** – Triggers an event to indicate a change from an AC power source to a battery power source.
- **Change to external power** – Triggers an event to indicate a change from a battery power source to an AC power source.
- **Low battery level** – Enables the threshold and reset threshold check boxes.
- **Threshold** – Defines the lowest specific battery level percentage that can be reached before an event is triggered.
- **Reset threshold** – Defines the specific low power value percentage that must be achieved before the low battery level threshold triggers another event. If the specific value remains below reset threshold, the monitor will not be triggered. For example, a low battery level threshold of 40% and a reset threshold of 60% would trigger an event when the battery level reaches 39%. In order for another event to be triggered, the battery level would have to reach 60% and then drop again to 39%.

Indicate the power settings you want to monitor.

Events

- Change to battery power
- Change to external power
- Low battery level

Threshold %

Reset threshold %

Polling interval Units



Reset thresholds values for percent and absolute values must be greater than the low power thresholds you define.

Process Monitor Settings

Supported client types – Windows Mobile Professional (excluding Windows CE), Windows Mobile Standard

Use a process monitor to evaluate changes on a list of processes on the client. A change is defined as a process being added to or removed from the list. Monitors may be most useful for capturing process activity for a process that runs without any user interface.



To monitor the start of one process and the stopping of another process, you need to create a separate monitor for each process.

Monitoring processes is distinct from monitoring applications use in the following ways:

- Processes do not always have the same name as their associated applications. A single application may have different ways of being invoked, which may result in different processes being launched. For example, you may be able to launch a calendar application by pressing a specific button on a handheld device or by navigating to the program file on the device's file system and running the file. These launch points may invoke different processes with different names, yet the resulting user experience may be the same.
- Processes do not always stop when the user chooses an application's exit command. The user experience may be that they have stopped using an application, but the associated process may remain on the process list because it is still running in the background.
- Administrators may want to consider using a window monitor instead of a process monitor if the intent is to monitor application use.

The following steps summarize the process monitor execution:

- 1 At client start up, a process monitor compiles a list of running processes to establish a baseline for the monitor.
- 2 At each defined polling interval, it compiles a new list of running processes and compares it to the baseline list. Processes that are new to the list are evaluated as "started" processes. Processes that are removed from the list are evaluated as "stopped" processes.
- 3 The monitor's defined action is executed according to the process list evaluation results.
- 4 The monitor uses the new list to replace the baseline list and waits for the next polling interval.

Administration > Policies and Profiles > New > Process Monitor > Process settings



- Click **Add** to indicate the process you want to monitor in the **Process Maintenance** dialog box and click **OK**. The name appears in the Process names portion of the wizard. Click **Add** to include additional processes.

Administration > Policies and Profiles > Monitors > New > Process Monitor > Process settings > Add



Wildcard usage: The **Process name** field accepts the use of the question mark (?) and asterisk (*) as reserved wildcard characters that perform a task on multiple files with similar names or extensions.

- **Edit** – Allows you to change the process you want to monitor using the Process Maintenance dialog box.
- **Delete** – Allows you to remove the selected process from the process monitor.
- **Started** – Triggers an event when the specified executable or process is started.
- **Stopped** – Triggers an event when the specified executable or process is stopped.

Substitution Variables

The following substitution variables are available:

- <MonitorData1> – Contains the event that caused the monitor to fire.
- <MonitorData2> – Contains the name of the process that generated the event.
- <MonitorData3>, <MonitorData4>, <MonitorData5> – Reserved for future use.

See ["Monitor Substitution Variables"](#) on page 319 to learn more.

Deployment and Usage Considerations

Shorter polling intervals produce the most accurate results; however, defining an appropriate polling interval requires that you consider the implications to your device's available resources and the likelihood of capturing the process event change. If the polling interval is too large, it is possible for the process to start and stop without the monitor detecting it. If the polling interval is too small, it may cause too much resource drain on the device, such as accelerated battery consumption.

Registry Monitor Settings

Supported client types – Windows Mobile Professional (excluding Windows CE), Windows Mobile Standard

Use the Registry Monitor Identification settings to watch for changes to specific data values under a defined registry key. Use the Filtering settings to trigger an event based on the nature of the change. DWORD and String data types are supported, and the Administrator should already know the data type to be used.

Administration > Policies and Profiles > New > Registry Monitor > Identity settings

- Key name** – Type a valid and properly formatted registry key name to monitor. Provide the full path in the registry to the key. A full path consists of the hive name, followed by one or more key names. Except for the last key in the path, the hive name and each key must be terminated by the backslash character (“\”).

Indicate the registry key and value you want to monitor.

Key name	HKLM\Software\Test
Value name (leave blank for default)	5

For the hive name, you can use the full hive name or the hive abbreviation, as shown in the following synonymous examples:

Example: HKLM\Software\MyCompany\mykey

Example: HKEY_LOCAL_MACHINE\Software\MyCompany\mykey\

<i>Hive abbreviation</i>	<i>Hive name</i>
HKCR	HKEY_CLASSES_ROOT
HKCU	HKEY_CURRENT_USER
HKLM	HKEY_LOCAL_MACHINE
HKU	HKEY_USERS
n/a	HKEY_CURRENT_CONFIG
n/a	HKEY_PERFORMANCE_DATA

- Value name** – Provide the name of a value to be monitored. Leave the name blank to monitor the default value.

Administration > Policies and Profiles > New > Registry Monitor > Filter settings

Indicate when you want the monitor to fire and reset.

Fire when condition met

Value type: **DWORD**

Numeric type: Hexadecimal Decimal

Fire when: **>=**

Value: **5**

Reset when: **<=**

Value: **4**

Sample for type DWORD

Indicate when you want the monitor to fire and reset.

Fire when condition met

Value type: **String**

Fire when: **!=**

Value: **5**

Reset when: **=**

Value: **5**

Sample for type String

- **Value type** – Select **DWORD** or **String**.
- **Fire when** – Choose the condition when the registry monitor is triggered.

Fire when

- !=
- <=
- >=
- Changed
- Deleted

DWORD operators

Fire when

- !=
- Changed
- Deleted

String operators

- **Value** – Type a valid numeric value based on the condition selected in the **Fire when** field.
- **Reset when** – Value is dynamically set based on the value in the **Fire when** field. You cannot edit this field.
- **Value** – Type a valid numeric value based on the condition set in the **Reset when** field.
- **Hexadecimal** – Accepts a 16-character base format using 0-9 and A-F.
- **Decimal** – Accepts a 0-9 numeric.

Custom Registry Monitor

You can also use the Registry monitor to create custom monitors for keys associated with your applications. Your application would deposit useful information in the registry in known locations. You can define a custom registry monitor to watch for changes and trigger actions accordingly.

Schedule Monitor Settings

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

The Schedule monitor lets you initiate events based on the calendar date and time on the client's device. You define when the schedule begins, as well as optional frequency of recurrence and date range during which the schedule is in effect.



- All schedules are based on the local date and time of the client.
- Schedule behavior varies between Windows Mobile, Symbian, and Blackberry devices. Be sure to verify expected schedule behavior for your device type.

Monitor “Default Policies Schedule”

The Default Policies Schedule monitor is a system-defined monitor related to policy management. The system pairs it with the Apply Policies action type and assigns it to or removes it from profiles, as appropriate, based on the presence or absence of specific policy types. You can edit its settings, but you cannot delete the monitor.

Schedule Type Settings

Use the type settings to establish the schedule monitor's frequency. Each type of schedule has different settings you configure.

Administration > Policies and Profiles > New > Schedule Monitor > Type

- **Daily** – Runs on a day-based schedule at a specific time. The schedule can run on a cycle of days or on selected days of each week.
- **Weekly** – Runs on a week-based schedule at a specific time. The schedule can run on a cycle of weeks for selected days of the week.
- **Monthly** – Runs on a month-based schedule at a specific time. The schedule can run on one or more days for selected months.
- **One time** – Runs only at the starting date and time you specify.

Select the type of schedule.

Perform this task

- Daily
- Weekly
- Monthly
- One time only

Schedule Start Settings – Daily, Weekly, Monthly

Use the Start settings to define the **Start time** (time of day) when the scheduled event begins, as well as the daily, weekly, or monthly frequency of recurrence.

Daily Recurrence Options

Administration > Policies and Profiles > Schedule Monitor > Daily > Start

For daily schedules, select one of the following recurrence options:

- **Cycle** – Select the daily frequency, which will start the scheduled event **Every n day(s)**. For example, if you select a cycle of 3, the schedule will start every third day.
- **Selected days** – Select the days of the week when the scheduled event will occur.

The screenshot shows the 'Start' settings for a 'Daily' recurrence type. The 'Type' dropdown is set to 'Daily'. The 'Start time' is set to '12:00:00 PM'. The 'Cycle' option is selected, with 'Every 1 day(s)'. The 'Selected days' section is also selected, with checkboxes for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday, all of which are checked.

Weekly Recurrence Options

Administration > Policies and Profiles > Schedule Monitor > Weekly > Start

For weekly schedules, select from the following recurrence options:

- **Every n week(s)** – Select the weekly frequency to start the event. For example, if you select a cycle of 3, the schedule will start every third week.
- **On the following days** – Select the days of the week when the scheduled event will occur. For example, if you select Monday and Friday with a cycle of every third week, the schedule will start every Monday and Friday of every third week.

The screenshot shows the 'Start' settings for a 'Weekly' recurrence type. The 'Type' dropdown is set to 'Weekly'. The 'Start time' is set to '6:00:00 AM'. The 'Every 1 week(s)' option is selected. The 'On the following days' section is selected, with checkboxes for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. Sunday, Thursday, and Saturday are checked.

Monthly Recurrence Options

Administration > Policies and Profiles > Schedule Monitor > Monthly > Start

For monthly schedules, select from the following recurrence options:

- **On the following day(s)** – Select the days during the month when the schedule starts. You can choose specific days from a calendar, or a day’s relative position within a month, e.g., “The last Saturday” of the month.

When selecting **Day(s) of the month**, if the day does not exist in a month, the schedule will begin on the last day of that month.

The screenshot shows the 'Start' tab of the configuration window. It includes a 'Type' dropdown set to 'Monthly', a 'Start time' field with '6:00:00 AM', and two main sections: 'Of the following day(s)' and 'Of the following month(s)'. In the first section, 'Day(s) of the month' is unselected, 'The' is selected with a dropdown set to 'Last', and another dropdown is set to 'Saturday'. In the second section, a grid of checkboxes for each month (January through December) is shown, with all boxes checked.

- **Of the following month(s)** – Select which months during the year the schedule will begin.

Common Schedule Start Options – Daily, weekly, and Monthly

Administration > Policies and Profiles > Schedule Monitor > Start

For daily, weekly, and monthly schedules, you can select the following additional options to control how the schedule starts:

- **Run at startup if schedule was missed** – Select to run a schedule at start up if the scheduled event did not run at the time defined by the schedule. For example, if the monitor process on the client is terminated and restarts after the scheduled event, the monitor will run the event if this option is selected.

The screenshot shows a checkbox labeled 'Run at startup if schedule was missed' which is checked. Below it, the text 'Randomize start time by' is followed by a numeric input field containing '120' and a unit dropdown menu set to 'Minutes'.



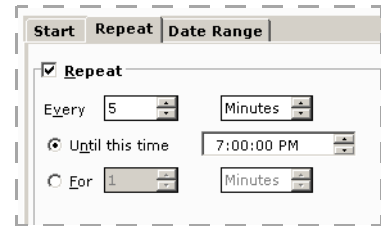
- If multiple scheduled events have been missed, the scheduled event will only run once at startup.
- When initially deploying a profile to a client, using this option does not run events scheduled in the past.
- This option applies only to missed scheduled events, not missed repeated events. See [“Schedule Repeat Settings – Daily, Weekly, Monthly”](#) on page 340.
- **Randomize start time by** – Use of this option results in a random amount of time added to a scheduled event start time. The random amount of time added will not exceed the value specified. By using this option you can distribute events for groups of clients across an event time window, rather than running all events simultaneously.

Schedule Repeat Settings – Daily, Weekly, Monthly

Use the **Repeat** settings to run multiple iterations of the event initially started by the schedule.

Administration > Policies and Profiles > Schedule Monitor > Repeat

- **Repeat** – Select to enable multiple iterations of the scheduled event. An event can never repeat for more than 24 hours.
- **Every *n* Minutes / Hours** – Defines the repeat frequency for the event.
- **Until this time** – Defines when event repetition will cease as a time of day. If this time of day is earlier than the event start time, repetition will continue until the following day.
- **For *n* Minutes / Hours** – Defines when event repetition will cease as period of time relative to the initial scheduled start time.



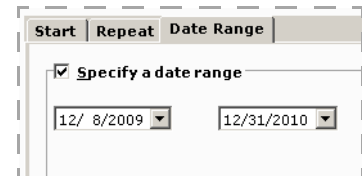
The screenshot shows a dialog box with three tabs: 'Start', 'Repeat', and 'Date Range'. The 'Repeat' tab is active. It contains a checked checkbox labeled 'Repeat'. Below it, there are three options: 'Every' with a value of '5' and a unit of 'Minutes', 'Until this time' with a value of '7:00:00 PM', and 'For' with a value of '1' and a unit of 'Minutes'. The 'Until this time' option is selected with a radio button.

Schedule Date Range Settings – Daily, Weekly, Monthly

Use the **Date Range** settings to define a range of dates during which the schedule monitor will run events. If you do not specify a date range, the monitor will always be active.

Administration > Policies and Profiles > Schedule Monitor > Date Range

- A schedule monitor will become active at 12:00:00 AM on the begin date.
- A schedule monitor will become inactive at 11:59:59 PM on the end date.



The screenshot shows a dialog box with three tabs: 'Start', 'Repeat', and 'Date Range'. The 'Date Range' tab is active. It contains a checked checkbox labeled 'Specify a date range'. Below it, there are two date pickers: the first is set to '12/ 8/2009' and the second is set to '12/31/2010'.

One-Time Schedules

Administration > Policies and Profiles > Schedule Monitor > One Time

A one-time schedule runs only a single time at the starting date and time you specify. Select from the following options:

- **Immediately** – The schedule runs immediately after being deployed to the client.
- **On earliest day at specified time** – The schedule runs at the next occurrence of the specified time after being deployed to the client.
- **At specified date/time schedule** – The schedule runs at the specified date and time. When running at a specified date and time, you can choose from the following additional options:
 - **Run at startup if schedule was missed** – Select to run at start up if the scheduled event did not run at the time defined by the schedule. For example, if the monitor process on the client is terminated and restarts after the scheduled event, the monitor will run the event if this option is selected.

Type
One time

Start

Run

Immediately

On earliest day at specified time

At specified date/time schedule

Run at startup if schedule was missed

Run immediately if deployed after schedule

Start time Start date

12:00:00 PM 7/ 9/2008

Randomize start time by

90 Minutes



When initially deploying a profile to a client, use of the **Run at startup if schedule was missed** option will not run events scheduled for a date that has passed.

- **Run immediately if deployed after schedule** – Select to run the event immediately upon deployment if the scheduled date and time are in the past.
- **Start time** – Defines the time of day when the scheduled event begins.
- **Start date** – Defines the date when the scheduled event begins.
- **Randomize start time by** – Use of this option results in a random amount of time added to a scheduled event start time. The random amount of time added will not exceed the value specified. By using this option you can distribute events for groups of clients across an event time window, rather than running all events simultaneously.

Substitution Variables

The following substitution variables are available when using the Schedule monitor:

- <MonitorData1> – Contains the schedule type, either “Daily Schedule” or “Weekly Schedule”, “Monthly Schedule”, or “One Time Schedule”.
- <MonitorData2> – Provides the local date and time on the client that the scheduled event ran. Note that this time will differ from the scheduled event time if the schedule is configured to run an event after a client misses it, and the client does fail to run the scheduled event.
- <MonitorData3> – Provides the repeat iteration count for the event. For the initially scheduled event, the iteration count is zero; for each subsequent iteration the count increases by one.
- <MonitorData4> – Contains the value “Was Missed” when the event was a missed scheduled event; contains an empty string in all other instances.
- <MonitorData5> – Reserved for future use.

See [“Monitor Substitution Variables” on page 319](#) to learn more.

Afaria Client Connection Considerations

When pairing a schedule monitor with a profile action that relies on an active connection, e.g., running a channel, ensure that a default connection is available on the client or create a profile action that establishes an active connection. See [“Profile – Client Actions” on page 233](#) to learn more about profile actions.

Channel Viewer LAN mode Considerations

When in the LAN mode in Channel Viewer, a connection is possible from the Afaria Client, but only if your computer’s operating system provides the connection.

Channel Viewer Dial-Up Mode Considerations

When in Dial-Up mode in Channel Viewer, a connection is possible from the Afaria Client, but only if the client’s ethernet or dial-up hardware is functional. If a connection is created by your computer’s operating system, then the connection mode selected in the Afaria Channel Viewer is not relevant when using dial-up networking—Afaria will not achieve a connection.

A dial-up connection initiated by the Afaria Client is distinguished from your computer’s operating system connection by the type of dialog box displayed.

- Afaria-Client-initiated connection – The dialog box is titled, “Establishing a Dial-Up Connection”, and is informational only.

- Operating system connection – There are numerous titles for the connection dialog boxes used when your computer’s operating system makes a connection (e.g., “Connect To” or “Dial-Up Connection”), and these dialog boxes are interactive.

Schedule Monitor Deployment Considerations

Consider the following when using Schedule monitors:

- Any change to a schedule monitor, except for the name and description, results in a new deployment of the monitor to clients. A new deployment is treated as an initial deployment of the schedule, thereby cancelling any queued retry or repeat events.
- Modifying an expired, one-time schedule results in the schedule running again on all clients.

Deploying Schedule Monitors in New Client Packages

Supported clients – Windows Mobile Professional, Windows Mobile Standard

Schedule monitors are eligible to become seed data when you use the Afaria Create Client Installation program to create new client packages. Clients are seeded with all schedule monitors that are enabled in all profiles to which they are assigned. At the time you create the client package, a client’s profile assignments include:

- Profiles that include the All Clients group assignment.
- Profiles that include any of the static client groups that you select for the client while creating the client package.

Window Monitor Settings

Supported client types – Windows Mobile Professional (excluding Windows CE), Windows Mobile Standard

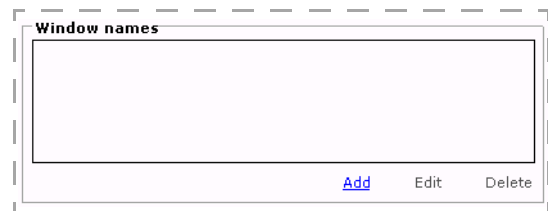
Use the window settings to watch for the creation or destruction of a specific window.



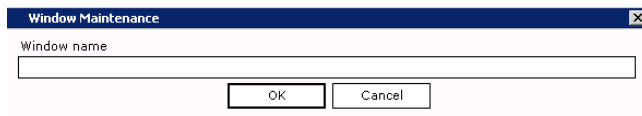
Only top-level windows on your desktop are monitored.

Administration > Policies and Profiles > New > Window Monitor > Windows settings

- Click **Add** to indicate the window you want to monitor in the **Window Maintenance** dialog box and click **OK**. The name you type appears in the Window names portion of the wizard.



Click **Add** to include additional window names.



- **Created** – Causes the monitor to indicate the creation of the specified window.
- **Destroyed** – Causes the monitor indicate the destruction of the specified window.



To monitor the creation of one window and the destruction of another window, a separate monitor is needed for each.

Channel Replication

Replication is a tool for using a single Afaria Server to manage channels for one or more other Afaria Servers. In the context of replication, the single, managing server is referred to as the source server and the other servers are referred to as the target servers.

The source server may be in a main-to-farm relationship or a peer-to-peer relationship with the target servers. A main-to-farm relationship is one in which the source and target servers operate as a single Afaria entity, sharing a single Afaria database. A peer-to-peer relationship is one in which the source and target servers operate as separate Afaria entities, each using their own Afaria database.

Channels are replicated from the source server to the target servers in a read-only state. In the farm relationship, the target servers are not able to create any channels on their own. In the peer-to-peer relationship, the target server may create and manage channels additional to those replicated from the source server.

Replication differs from importing and exporting channels. Once an Afaria Server exports channels, the server retains no further control over the channels. When an Afaria Server imports channels, the server takes complete ownership of the channels and is able to exercise any channel management tasks over them.



- Due to its role as the only source server for channel replication in a server farm, a main server is the only server in a farm with access to the replication feature.
- If you have a both a test Afaria Server where you create channels and a production Afaria Server where you publish channels, you should use the import/export feature to move channels between these servers.

Group Profiles and Replicated Channels

Profiles are the vehicles for distributing channel and channel set tasks to client devices; channels and channel sets are components in the profile's definition. Server farm replication servers that are using replicated channels use the main server's profiles. Peer Afaria Servers that are using replicated channels are responsible for managing their own profiles.

See ["Managing Profiles" on page 225](#).

Administration > Replication

Replication	Replication sets				
<ul style="list-style-type: none">Replication sets<ul style="list-style-type: none">ConfigurationInventorySoftwareServers<ul style="list-style-type: none">FSAll	<table border="1"><thead><tr><th>Name</th></tr></thead><tbody><tr><td>Configuration</td></tr><tr><td>Inventory</td></tr><tr><td>Software</td></tr></tbody></table>	Name	Configuration	Inventory	Software
Name					
Configuration					
Inventory					
Software					

Left panefolders:

Replication sets. Replication sets are sets of channels that you create to replicate to other Afaria Servers. These sets can include any or all of the channels you have created in Channel Administration.

Servers. The Afaria Servers listed in this folder are the servers with which you have registered. Depending on your server environment (peer-to-peer or server farm), you can replicate channels to or from any server in this list.

These folders are empty until you create replication sets and add servers. You cannot delete or rename these folders. Once you have created a replication set or added a server, the tabs that appear in the right pane will change.

Replication in a Server Farm Environment

In a server farm environment, target servers cannot create, publish, or replicate channels; they only display the channels created and published at the source server. The administrator at the source server must replicate its channels to the target servers in the farm. To ensure data consistency between all local servers in the server farm, the administrator at the source server should consistently replicate any channel updates or new channels to all of the local servers in the farm. To client users, the appearance is seamless; the source server's published channels will appear to users when they connect to any local Afaria Server.



Channel replication is supported only between same-version Afaria Servers.



Bandwidth throttling must be enabled on all Afaria Servers in a server farm environment if you intend to use bandwidth throttling features in any of the channels you replicate.

When you replicate channels to target servers in a server farm, you follow these steps:

Step 1: Create a replication set.

Step 2: Select to Auto advertise all items in the replication set.

Step 3: Assign the replication set to the target servers.

Step 4: Replicate the channels to the target servers.

Replication in a Server Peer Environment

Replicated channels appear in the Channels Administration area on the target server exactly as they do on the source server—except that you cannot edit these channels. You can publish or unpublish them for client users, but you cannot change any of the channels' properties.

You'll notice that when you view a replicated channel in Administration, the **Examine channel contents** link is the only available option on the Properties tab. You can click **Examine channel contents** to display a read-only version of the channel's contents in the channel-specific editor.

However, when Channel Viewer users view published, replicated channels, the channels appear to them exactly as they would if the channels had been created and published at the target server. If you enable authentication for any of your Windows clients, those clients are authenticated against the credentials on the source server, rather than against the credentials on the local Afaria Servers.

To replicate a channel from a source server *to* a target server, follow these general steps:

Step 1: Create a replication set.

Step 2: Select the channels you want to advertise.

Step 3: Register with the target server.

Step 4: Assign the replication set to the target server.

Step 5: Notify the server administrator at the target server that channels have been advertised for replication.

To replicate channels *from* a source server to your target server, follow these basic steps:

Step 1: Register with the source server.

Step 2: Select the channels to accept from the source server.

Step 3: Replicate the channels from the source server.



You can view information about replication activity for your Afaria Server in Data views, Logs.

Creating a Replication Set



You can only create replication sets in a peer-to-peer scenario, or if your Afaria Server is the source server in a server farm scenario.

Before you can replicate channels to another Afaria Server, you must create a replication set. You select the channels you want to be part of the set to advertise to other servers. You can assign more than one replication set to a server. If you are creating a replication set for target servers in a server farm, this replication set will probably include all the channels you have created in Channels Administration.

To create a replication set:



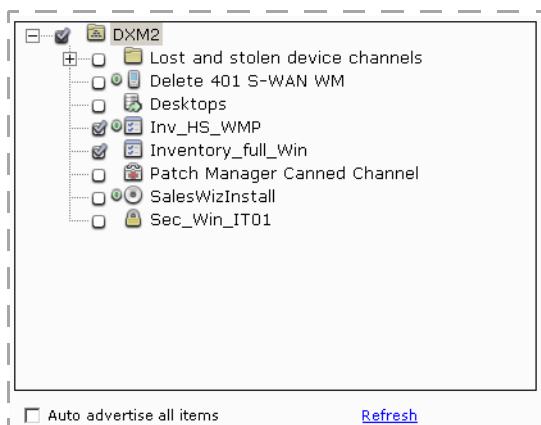
- 1 Click **New replication set** to open the New replication set dialog box.
- 2 Type a unique **Name** for the set and choose **OK**. The set displays on the Replication page in the left pane.

Once you have created a replication set, you can use the Advertise tab to select and advertise the channels that you want to include in the set. You can use the Assign tab to select the target servers for the set.

Advertising Channels for Replication

The **Advertise** tab includes a copy of the channels that appear on the Channel Administration page, only each item has a check box to the left of it.

Administration > Replication > *replication set* > Advertise



If you are replicating channels in a server farm scenario, you should select the **Auto advertise all items** check box. This ensures that all local Afaria Servers in the farm receive the source server's channels.

In a peer-to-peer scenario, you can select channels to advertise four ways. You can select the check box for:

- each channel you want to add to the replication set
- **Auto advertise all items** to add all channels and folders to the replication set
- a folder to add all channels in that folder
- the server to advertise all channels from your server.

You can click **Refresh** to refresh the channel list on the Advertise page and display any new channels that have been created on your server.

Once you have selected the channels you want to advertise, you are ready to assign the replication set to a server.

Assigning a Server to a Replication Set

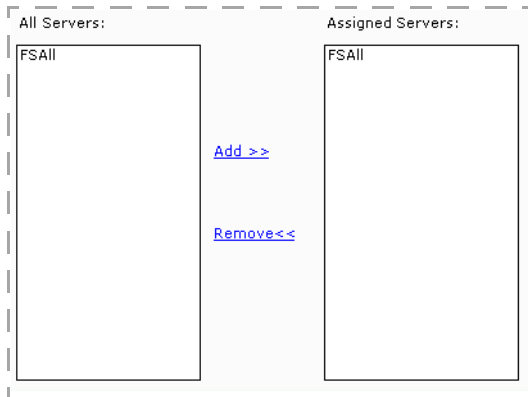
Once you have created a replication set and advertised the channels in that set, you can assign the replication set to a target server. Before you assign any replication sets, you must have registered with the target server so it appears in your servers list; if you are replicating to a target server in a server farm scenario, the target servers are automatically registered when they are installed, and will appear in your list.



For more information on registering with servers in a peer-to-peer scenario, "[Registering a Server](#)" on page 350.

When you click the **Assign** tab, the Assign page appears in the right pane.

Administration > Replication > replication set > Assign



On the Assign page, you select the servers to which you want to replicate channels from the **All Servers** list box and then click **Add**.



When you have advertised and assigned replication sets to any server in your list, you can click **Replicate to** on the toolbar, or right-click the server in the left pane and select **Replicate to** on the shortcut menu. This replicates the channels to the selected server; the channels appear on the Accept page at the target server. You should notify the server administrators at these servers when you have replicated channels. A message should also appear in the Data views, Logs folder at the target or local Afaria Servers.



In a peer-to-peer scenario, if the target server to which you are replicating channels is not licensed for a specific channel type, those channels will not be replicated to the target server.

Registering a Server

Afaria requires that source and target servers are registered with each other in order to engage in any shared replication activity. That is to say, a source server must register each of its target servers and a target server must register each of its source servers. In a peer-to-peer environment, you must manually register servers. In a server farm environment, all servers automatically register.

To register a server:



- 1 Click **New Server** to open the New Server dialog box.
- 2 Type an Afaria Server name, which does not have to be the same name as the original server, and the Afaria Server address, which can be a DNS host name or an IP address.

The server appears on the Channels Replication page in the left pane.

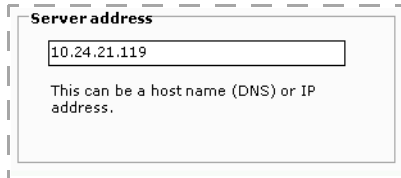
Once you have registered servers, use the following tabs to manage the replication relationship.

- **General** – Displays the address of the registered Afaria Server. See [“Viewing General Server Properties”](#).
- **Assign** – Lets you assign replication sets to registered target servers. See [“Assigning a Server to a Replication Set” on page 349](#).
- **Schedule** – Lets you define schedules for replicating to a target server and for replicating from a source server. See [“Setting a Replication Schedule” on page 353](#).
- **Accept** – Lets you accept advertised replication sets from a registered source server. See [“Accepting a Replication Set from a Source” on page 355](#).
- **Options** – Lets you define rules for replicating from source servers. See [“Setting Replication Options” on page 356](#).

Viewing General Server Properties

The General tab displays the registered Afaria Server DNS host name or IP address.

Administration > Replication > *registered server* > General



Server address

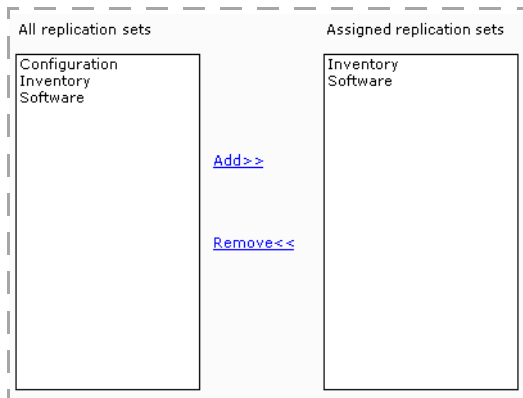
10.24.21.119

This can be a host name (DNS) or IP address.

Assigning a Replication Set to a Target

Assign a replication set to a registered target Afaria Server to enroll the target for synchronization action with the source. Assign a replication set to a registered target Afaria Server after you create a replication set and advertise the channels.

Administration > Replication > *registered server* > Assign



All replication sets

Configuration
Inventory
Software

Assigned replication sets

Inventory
Software

[Add>>](#)

[Remove<<](#)

The All replication sets list box displays all of the available replication sets on your server. To assign a replication set to the server you have selected in the left pane, you select the replication set and click **Add**.

The replication set you have added appears in the Assigned replication sets list box. To remove this set, you select it in the Assigned replication sets area and click **Remove**. The replication set will no longer be listed in the Assigned area.

Setting a Replication Schedule

You can set a schedule for replicating channels to and from other servers. For example, use this option when you regularly update channels that other servers will also need to publish. The Schedule page appears and contains the following options: **Replicate to** and **Replicate from**.

Administration > Replication > *registered server* > Schedule

The screenshot shows two sections: 'Replicate to' and 'Replicate from'. The 'Replicate to' section has a checked 'Enable schedule' checkbox and a 'Schedule...' link. The 'Replicate from' section has an unchecked 'Enable schedule' checkbox and a 'Schedule...' link.

You select the check box for the schedule type you want to create and click the **Schedule...** link to set the schedule properties.

Replication – Schedule Tab

The Schedule Editor's Schedule tab contains the following fields:

- **Name** and **Description**. System-defined fields to identify the schedule as a “replicate to” schedule or a “replicate from” schedule.
- **Schedule type**. Displays the type of schedule: Daily, Weekly, Monthly, Once, or Online. You can select a new schedule type from the drop-down list.
- **Start time**. You can use the spin box to change the start time. You can also select the option to Run at startup if schedule was missed, so the scheduled task will run when the service starts or when the client connects.
- **Schedule Task area**. Displays the options for the type of schedule selected:
 - For *Daily* or *Weekly* schedules, displays the days of the week.
 - For *Monthly* schedules, displays the months of the year.

The screenshot shows the 'Internet access parameters' section. It has two radio buttons: 'Monitor all Internet connections' (selected) and 'Monitor a specific Dial-up Networking connection'. Below the second radio button is a drop-down menu. There are two checked checkboxes: 'Don't run if less than 4 hour(s) and 0 minute(s) have elapsed since the last execution of this schedule.' and 'Delay connection by 1 minute(s)'. The numbers 4, 0, and 1 are in spin boxes.

Schedule type “online” - example properties

- For *Once* schedules, this field does not display any information.
- For *Online* schedules, displays the Internet access parameters.

To keep any changes you make to a schedule, you can click **OK** to save the changes and close the Schedule Editor, or you can click **Apply** and click the **Advanced** tab to continue editing the schedule.

Replication – Advanced Tab

Depending on the schedule type, the Schedule Editor's Advanced tab contains the following fields:



If you are editing a "Once" schedule, no fields appear on this page. If you are editing an "Online" schedule, only the **Specify a date range** field appears.

- **Specify a date range.** Displays the date range for this schedule. You can change the date range by selecting a new date from the **Begin** and **End** spin boxes.
- **Repeat.** Displays the parameters for repeating the scheduled task. You can edit any of the fields in this area.
- **Retry.** Displays the number of times Afaria should attempt to retry running the scheduled task. The **Retry interval** specifies the time period. You can edit either of these fields.
- **Randomize start time by.** Displays the parameters for randomizing the start time for the scheduled task. You can change the time by selecting values from the spin boxes.

You can specify a date range. If a date range is specified, this task will only run during this range. If no range is specified, the schedule is always active.

Specify a date range

Begin: 9/ 1/2008 End: 9/30/2008

Schedules can be set up to run at a specific time or on a recurring basis.

Repeat

Every: 15 Minutes

Until this time: 12:00:00 AM

For: 24 hour(s) 0 minute(s)

Retry: 0 time(s) Retry interval: 0 minute(s)

Randomize start time by: 0 hour(s) 0 minute(s)

Schedule type "daily" - example properties

To keep any changes you make to a schedule, you can click **OK** to save the changes and close the Schedule Editor, or you can click **Apply** and click the **Schedule** tab or the **Network** tab to continue editing the schedule.

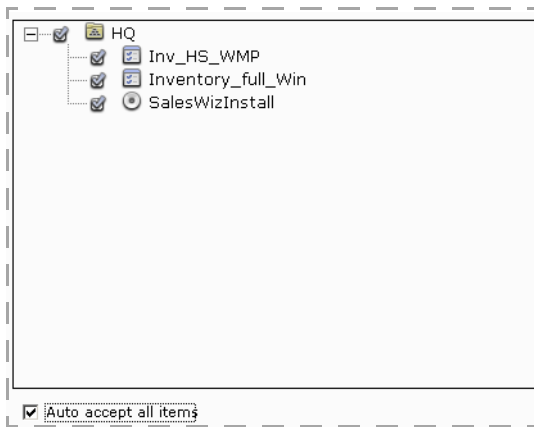
Accepting a Replication Set from a Source

When the Afaria Server administrator at a source server has advertised channels to your server, you can select which channels you want to accept on the Accept tab. Every time you accept items and replicate them from the source server, any new channels advertised by the source server will also appear on this page.



If the target server is not licensed for a specific channel type, the channels do not replicate and do not appear in the list on the Accept page.

Administration > Replication > *registered server* > Accept



In a server farm scenario, if you are replicating channels from the source server, you should select the Auto accept all items check box. this ensures you receive all the channels the source server has advertised to your server.

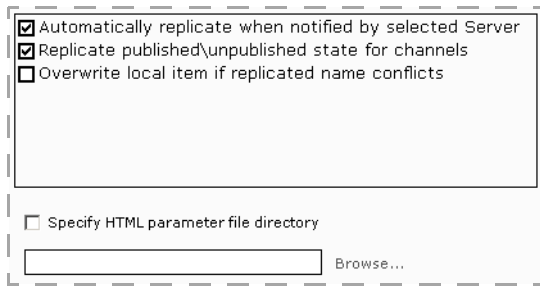


In a peer-to-peer scenario, you can select the check boxes next to channels you want to replicate, or select the **Auto accept all items** check box to accept all channels. When you've selected the channels to replicate, you can click the **Replicate from** icon on the toolbar, or right-click and select **Replicate from** on the shortcut menu. The replicated channels you selected appear on your Administration page. Any new channels advertised by the source server will appear on the Accept page.

Setting Replication Options

Use the options page to define rules for replicating from source servers.

Administration > Replication > *registered server* > Options



Automatically replicate when notified by selected Server
 Replicate published\unpublished state for channels
 Overwrite local item if replicated name conflicts

Specify HTML parameter file directory

Browse...

You can select one or more of the following options:

- **Automatically replicate when notified by selected Server.** Automatically replicates channels from the source server you have selected when it replicates channels to your target server. If you do not select this option, your server will not automatically receive replicated channels when the source server replicates to your server.
- **Replicate published\unpublished state for channels.** Replicates the channels in their unpublished or published state in Administration on the target server. Any published channels will run or appear to client users when they connect to the server.
- **Overwrite local item if replicated name conflicts.** Overwrites any channel with the same name that exists on the target server.

A channel name, in this context, is evaluated as its folder path plus the channel name. For example, a channel named “Hardware” stored in nested folders “Inventory\Windows” is evaluated as “Inventory\Windows\Hardware.” Copying channel “Inventory\All\Hardware” into folder “Inventory\Windows” results in the system renaming the channel during the copy to prevent a conflict with the other “Hardware” channel.

(Multitenancy) The overwrite action is valid only for overwriting channels in the same tenant. The replication fails if there is a channel conflict in another tenant.

If any parameter files are associated with the channels, you must select the **Specify HTML parameter file directory** check box and enter the directory location, or click **Browse...** to navigate to it.



For Software Manager channels, the parameter file includes both the XEC file and the SWM file. During replication, these files are placed in the following location on target servers in a server farm environment, no matter where the file resides on the source server:

Program Files\Afaria\Data\Channel\HTML*.xec

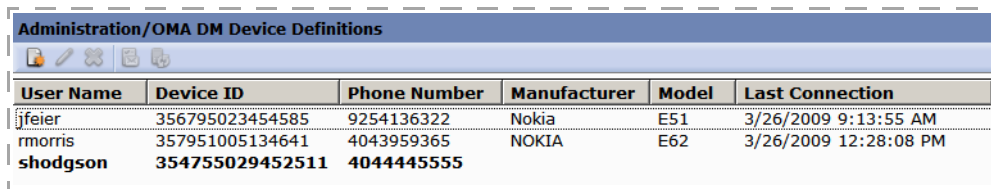
OMA DM Device Definitions

Use the Open Mobile Alliance (OMA) Device Management (DM) Definitions area of Afaria Administrator to turn your OMA-DM-enabled devices into Afaria's OMA DM Clients. See ["Creating OMA DM Clients" on page 65](#) for more information about prerequisites and managing OMA DM Clients.

Complete the following work flow on the OMA DM Device Definitions page to turn a device into an OMA DM Client:

- 1 Use the OMA DM Device editor to create a device definition that includes the device's IMEI number and phone number.
- 2 Issue the command to provision a device with the initial settings for device management.
- 3 Issue the server notify command to initiate a client connection to the OMA DM server. Clients receive their assigned profile and any associated policies during the session.

Administration > OMA DM Device Definitions



User Name	Device ID	Phone Number	Manufacturer	Model	Last Connection
jfeier	356795023454585	9254136322	Nokia	E51	3/26/2009 9:13:55 AM
rmorris	357951005134641	4043959365	NOKIA	E62	3/26/2009 12:28:08 PM
shodgson	354755029452511	4044445555			

Creating a Device Definition

Create an OMA DM device definition to establish a record for a device that you plan to manage with Afaria's OMA DM features. The OMA DM server runs sessions only with OMA DM devices that it can associate with a device definition. Begin on the OMA DM Device Definitions page.



- 1 Click the **New device** icon on the page's toolbar.
- 2 Define the device's basic attributes:
 - Device ID – The device's IMEI number. Use a device's IMSI number if an IMEI number is not available.
 - Phone number – The device's phone number as contiguous digits, without special characters or spaces, including any leading international dialing digits that your SMS messaging provider may require.
 - User name – The device's user name, as defined on the device.

- 3 Define credentials for both the OMA DM server and the OMA DM device to use for authentication with each other. Users are not required to know these credentials.



The screenshot shows a form with two main sections: 'Server' and 'Client'. Each section has a 'Password' field with a 'Random' button and a 'Nonce' field. The 'Server' section shows a password of 'AY1ax9oTYATjvZ' and a nonce of 'XdopYD4oSJdSAsRJq58p+Q=='. The 'Client' section shows a password of 'Mc1U2ZsOZbZFKi' and a nonce of 'G4PvpiESi/YB+u1SZI3SVA=='. The form is enclosed in a dashed border.

- Password – User-defined password. Choose **Random** to have the system generate a password for you.
- Nonce – Number-used-once (nonce) value. The system generates this value for you. The value is replaced with a new value after each server-client connection.

- 4 (Optional) Include a provisioning command or a server notify command. See [“Provisioning a Device”](#).

The provisioning and server notify options are enabled only when your Afaria SMS gateway is configured for operations. See [“SMS Gateway” on page 144](#).

- 5 Choose **OK**.

Provisioning a Device

Provisioning a device configures it for making connections with the Afaria OMA DM server. Provisioning commands are embedded in SMS messages and sent to the device via the Afaria Server SMS gateway. Device users must open the message and save the settings to affect the provisioning. You must advise users on their role.



- 1 Select one or more devices from the OMA DM Device Definitions page and choose **Provision device** or select the provision option prior to saving a device definition.
- 2 (Optional) To prompt the device user for a PIN required by the network for authentication, select the User PIN option and provide the PIN. A single user PIN is used for multiple devices. Notify users of the PIN value.
- 3 (Optional) To send a client connection command with the provision command, select the connect to server option. The client connection command causes the device to connect to the OMA DM server as soon as provisioning is complete.
- 4 Choose **Send** to send the provisioning message. Device users must open the message and save the settings to the device.

Initiating a Client Connection

Initiate a client connection to the OMA DM server by issuing a server notify command. Server notify commands are embedded in SMS messages and sent to the device via the Afaria Server SMS gateway.



- 1 Select one or more devices from the OMA DM Device Definitions page and choose **Send server notify to device**.

The user must interact with the device to authorize the connection to the OMA DM server unless you have established a trust relationship for the client/server connections. See [“OMA DM task – Trust” on page 261](#).

Outbound Notifications

An outbound notification is a set of instructions that is sent from an Afaria server to a client. The instructions tell the client to initiate a connection back to its server to run a session. To send the notification, the server must use a client's IP or SMS address.

The outbound notification feature for Afaria clients requires that a "listener" is present at the client. The server delivers the listener to the client during the client's first connection. Therefore, a client must have had at least one successful Afaria connection before the client can receive an outbound notification.

Afaria includes a public Web service for the outbound notification feature so that you can offer the service without requiring access to your Afaria Administrator server. See *Afaria Reference Manual | APIs*.

Managing client outbound notification addresses

Manage outbound notification addresses prior to sending outbound notifications. You can supply a specific IP or SMS address for a client. By default, the server uses a client's last-known address.

- 1 On the Client groups page, select a group or select one or more clients.
- 2 Choose **Client connection information**.
- 3 If the **Last known IP value** is not current or is unknown, update the **User IP address** or **SMS address** for the Client.

- Client name – The assigned name of the Client device.
- Last known IP – The Client IP address the server recorded during the last Client connection.
Afaria uses this value for sending outbound notification if the user IP and SMS values are left blank. The value "Unknown" is appropriate for Clients that support SMS notifications but not IP notifications.
- User IP address – An IP address to use to connect to the Client. If defined, this value overrides the **Last known IP** value for making an outbound notification.
- SMS address – An SMS address to contact Clients that support SMS. If defined, this value overrides the IP values for making an outbound notification.

The server sends future notifications using any overrides you defined and using last-known addresses for Clients without overrides.

Sending an Outbound Notification to Run a Channel

This feature is available on Client Groups, Policies and Profiles, and Data Views Clients pages.

Send an outbound notification to run a channel to a client when you want the client to connect to an Afaria Server right away to request a specific channel. To run, the channel must be included in one of the client's group profile allowed channels list.

These steps describe the task from the Client Groups page. However, the steps are similar from the other pages:

- 1 On the client groups page, select a client group in the left pane or one or more clients in the right pane.
- 2 Right-click and select **Outbound notification > Run Channel**.
- 3 Select a published channel that supports the client type for your selection.
- 4 Choose **OK** to send the notification.

If notification was successful, the client attempts to connect to the server and request the selected channel. The Messages log captures the success or failure of sending the outbound notification.

Sending an Outbound Notification to Apply Policies

This feature is available on Client Groups, Policies and Profiles, and Data Views Clients pages.

Send an outbound notification to apply a policy to a client when you want the client to connect to its server right away to receive its group profile and associated policies.

These steps describe the task from the Client Groups page. However, the steps are similar from the other pages:

- 1 On the Client groups page, select a Client group in the left pane or one or more Clients in the right pane.
- 2 Right-click and select **Outbound notification > Apply Policies**.
- 3 Choose **OK** to send the notification.

If notification was successful, the client attempts to connect to the server. The Messages log captures the success or failure of sending the outbound notification.



Data views

Data views provides a variety of ways for you to view and manage client information and logs. Clients view presents information by client instead of component. You can view client data in predefined views, or create custom folders, views, groups, and SQL views.

This chapter covers these topics:

- [“Database schemas” on page 363](#)
- [“Creating Custom Database Views” on page 389](#)
- [“Managing Client Data” on page 395](#)
- [“Working with Logged Actions” on page 439](#)
- [“Working with Client Inventory Data” on page 452](#)
- [“Track Software Manager channels” on page 467](#)
- [“Restore backed up client data” on page 477](#)
- [“Tracking Software Compliance and Usage Data” on page 482](#)
- [“Viewing client patch information” on page 487](#)
- [“View client deployment information” on page 492](#)

Database schemas

To understand how the various “parts” of our database work together you should become familiar with the terms that represent those parts.

- **Schema** represents a group of similar classes that share a common theme, such as the BlackBerry schema.
- **Class** represents a group of similar properties included in a unique database table, such as A_INV_DEVICE.
- **Property** represents a specific piece of information stored by a database column, such as BatteryLevel, SerialNumber, DeviceName, etc.

Classes are children of schemas and properties are children of classes. A class can be the child of multiple schemas; a property can be the child of multiple classes.

You access the schemas, classes, and properties when you query inventory, log, and server-related information through the view editor when creating custom views. The classes and properties display in plain language. For example, the A_INV_DEVICE class displays as Device, and the BatteryLevel property displays as Battery Level. Providing you the view editor to query table information allows us to make changes to the database without affecting the custom queries you create.

Inventory schemas

Most of the schemas in the Add column dialog box above provide access to inventory classes and are specific to a client's client type.



Phone and network data collected and reported by Inventory Manager varies by device type. See “Collecting phone and network data on handhelds” located in the *Afaria Reference Manual | Components* for information on phone data collected from clients.

BlackBerry schema

<i>Class</i>	<i>Property description</i>
BlackBerry	<p>Provides information about the device, including:</p> <ul style="list-style-type: none"> • area identifier • base identifier • country name in which the device is currently located • current network that links the device to your computer system • default network that links the device to your computer system • disk space free in kilobytes • whether the device was in/out of the holster at the time of the inventory scan • home country name or name in which the device is based • date the operating system (OS) was installed • total program execution stack amount • message key • Mobitex access number of the device • total number of networks available to this device • whether the power save mode has been activated • product version • whether the device was ON • strength/weakness of the signal was at the time of the scan • whether the device was active or inactive • reason the scan was performed • version of the operating system software development kit • whether the security status was enabled or disabled
BlackBerry	<ul style="list-style-type: none"> • an amount used in the program execution stack (last-in, first-out (LIFO) stack used to store program variables and state information as the system is operating) • a counter that indicates how long the device has been active on the network • total memory in kilobytes • total number of messages stored on the device • whether the device can transmit • number of unread messages stored on the device • Client user's E-mail address • wireless network being used by the device
Database	<p>Provides information about the database used by the device, including:</p> <ul style="list-style-type: none"> • name • record used • size
Device	<p>Provides device-specific information about the device, including:</p> <ul style="list-style-type: none"> • amount of battery remaining • compile date for the client • name • model • operating system • version of the operating system • last date the inventory was scanned • serial number • user name of the person using the device

<i>Class</i>	<i>Property description</i>
Memory	Provides information about memory on the device, including: <ul style="list-style-type: none">• available memory in kilobytes• name of the memory card• total memory in kilobytes
Phone	Provides information about phone properties available on the device, including: <ul style="list-style-type: none">• International Mobile Equipment Identifier (IMEI)• International Mobile Subscriber Identifier (IMSI)• status (on, off)• supported (yes, no)
Software	Provides information about software installed on the device, including: <ul style="list-style-type: none">• number of associated records of the software installed• names of the software installed• file sizes of the software installed

Palm schema

<i>Class</i>	<i>Property description</i>
Device	Provides information about the Palm handheld, including: <ul style="list-style-type: none">• battery amount remaining• compile date for the client• IMEI (for wireless devices on GSM networks like the Palm Treo)• name• model• operating system• version of the operating system• last date the inventory was scanned• serial number• user name of the person using the Palm handheld
Memory	Provides information about the memory on the Palm handheld, including: <ul style="list-style-type: none">• available memory in kilobytes• name of the memory mechanism (Card 0, Card1)• total memory in kilobytes
Palm	Provides information about the Palm handheld's display, including: <ul style="list-style-type: none">• whether the handheld has a color display• whether the handheld displays horizontal pixels• whether the handheld displays vertical pixels
Palm Card	Provides information about the removable card used by the Palm handheld, including: <ul style="list-style-type: none">• class• manufacturer• type• product name• number of slots• identification number• total memory in kilobytes• used memory in kilobytes
Phone	Provides information about phone properties available on the Palm handheld, including: <ul style="list-style-type: none">• current mobile operator• current network – network provider• International Mobile Equipment Identifier (IMEI)• International Mobile Subscriber Identifier (IMSI)• phone number• status (on, off)• supported (yes, no)
Software	Provides information about software installed on the Palm handheld, including: <ul style="list-style-type: none">• identification of the software creator• names of the software installed• file sizes of the software installed• software versions of the software installed

Windows Mobile Professional schema

Class	Property description
Bluetooth	Provides information about the Bluetooth data used on the device, including: <ul style="list-style-type: none"> connectable (yes, no) device address (device name/address) discoverable (yes, no) status (on, off) supported (yes, no)
Custom Data folder Custom Name view Custom Value view	Allows you to create one or more unique registry key name and value, which can then be included in custom views in Data views, Clients and Inventory. Create the string or dword key name and value in the Custom Fields folder (which you must also create) under HKLM\SOFTWARE\Afaria\Afaria\Client\Inventory\Custom Fields. You can create the key name and value via a Session Manager channel or manual entry.
Device	Provides information about the device, including: <ul style="list-style-type: none"> battery amount remaining compile date for the client name operating system version of the operating system processor type last date the inventory was scanned serial number^a user name of the person using the device
IrDA	Provides information on Infrared Data Association (IrDA) on the device, including: <ul style="list-style-type: none"> status (on, off) supported (yes, no)
Memory	Provides information about the memory on the device, including: <ul style="list-style-type: none"> available memory in kilobytes name of the memory mechanism (Card 0, Card1) total memory in kilobytes
Phone	Provides information about phone properties available on the on the device, including: <ul style="list-style-type: none"> current mobile operator current network - network provider International Mobile Equipment Identifier (IMEI) International Mobile Subscriber Identifier (IMSI) phone number status (on, off) supported (yes, no)
Removable	Provides the visible and invisible name of the removable card used by the device.
Software	Provides information about software installed on the device, including: <ul style="list-style-type: none"> names of the software installed file sizes of the software installed software versions of the software installed

<i>Class</i>	<i>Property description</i>
WiFi	Provides information about Wireless Fidelity (WiFi) network capabilities available on the device, including: <ul style="list-style-type: none">• supported (yes, no)• status (on, off)• MAC address (for WiFi filtering purposes)• network name/access point
Windows CE	Provides assorted information about the device, including: <ul style="list-style-type: none">• whether the device includes a backup battery• whether the device has a color display• name of the company that owns the device• language that displays on the device• model• iPAQs <i>only</i> display the iPAQ model in Device Model• description of the expansion pack (flash or removable cards: flash cards indicate the total memory and the available memory in kilobytes; removable cards indicate the card name)• whether the device has an external battery• battery power remaining on the external battery• whether the device displays horizontal pixels• maker of the device• individual that owns the device• version of the device's installed ROM• Client user's telephone number• Client user's E-mail address• whether the device displays vertical pixels

a. For some Symbol devices, the serial number field may return the device's UUID.

Windows Mobile Standard schema

<i>Class</i>	<i>Property description</i>
Bluetooth	Provides information about the Bluetooth data used in the device, including: <ul style="list-style-type: none"> • connectable (yes, no) • device address (device name/address) • discoverable (yes, no) • status (on, off) • supported (yes, no)
Custom Data folder Custom Name view Custom Value view	Allows you to create one or more unique registry key name and value for the device, which can then be included in custom views in Data views, Clients and Inventory. Create the string or dword key name and value in the Custom Fields folder (which you must also create) under HKLM\SOFTWARE\Afaria\Afaria\Client\Inventory. You can create the key name and value via a Session Manager channel or manual entry.
Device	Provides information about the device, including: <ul style="list-style-type: none"> • battery amount remaining • compile date for the client • IMEI (only populated for signed, wireless devices on GSM networks, and may require a privileged certificate to retrieve) • name • operating system • version of the operating system • processor type • last date the inventory was scanned • serial number • user name of the person using the device
IrDA	Provides information on Infrared Data Association (IrDA) on the device, including: <ul style="list-style-type: none"> • status (on, off) • supported (yes, no)
Memory	Provides information about the memory on the device, including: <ul style="list-style-type: none"> • available memory in kilobytes • name of the memory mechanism (Card 0, Card1) • total memory in kilobytes
Phone	Provides information about phone properties installed on the device, including: <ul style="list-style-type: none"> • current mobile operator • current network – network provider • International Mobile Equipment Identifier (IMEI) • International Mobile Subscriber Identifier (IMSI) • phone number • status (on, off) • supported (yes, no)
Removable	Provides the visible and invisible name of the removable card used by the device.
SIM	Provides information about the phone number on the device.

<i>Class</i>	<i>Property description</i>
Smartphone	<p>Provides assorted information about the device, including:</p> <ul style="list-style-type: none">• whether the device includes a backup battery• whether the device has a color display• name of the company that owns the device• language that displays on the device• model• description of the expansion pack (flash or removable cards: flash cards indicate the total memory and the available memory in kilobytes; removable cards indicate the card name)• whether the device has an external battery• battery power remaining on the external battery• whether the device displays horizontal pixels• maker of the device• individual that owns the device• version of the device's installed ROM• Client user's telephone number• Client user's E-mail address• whether the device displays vertical pixels
Software	<p>Provides information about software installed on the device, including:</p> <ul style="list-style-type: none">• names of the software installed• file sizes of the software installed• software versions of the software installed
WiFi	<p>Provides information about Wireless Fidelity (WiFi) network capabilities installed on the device, including:</p> <ul style="list-style-type: none">• supported (yes, no)• status (on, off)• MAC address (for WiFi filtering purposes)• network name/access point

Symbian schema

<i>Class</i>	<i>Property description</i>
Bluetooth	Provides information about the Bluetooth data used on the device, including: <ul style="list-style-type: none">• connectable (yes, no)• device address (device name/address)• discoverable (yes, no)• status (on, off)• supported (yes, no)
Device	Provides information about the Symbian device, including: <ul style="list-style-type: none">• battery amount remaining (90, 5, and 1: 90 = Good, 5 = Low, 1 = Not Supported)• compile date for the client• IMEI (for wireless devices on GSM networks)• name• model• operating system• version of the operating system• last date the inventory was scanned• serial number• user name of the person using the Symbian device
IrDA	Provides information on Infrared Data Association (IrDA) on the device, including: <ul style="list-style-type: none">• status (on, off)• supported (yes, no)
Memory	Provides information about the memory on the Symbian device, including: <ul style="list-style-type: none">• available memory in kilobytes• name of the memory mechanism (Card 0, Card1)• total memory in kilobytes
Phone	Provides information about phone properties installed on the Symbian device, including: <ul style="list-style-type: none">• current mobile operator• current network – network provider• International Mobile Equipment Identifier (IMEI)• International Mobile Subscriber Identifier (IMSI)• phone number• status (on, off)• supported (yes, no)
Software	Provides information about software installed on the Symbian device, including: <ul style="list-style-type: none">• names of the software installed• file sizes of the software installed
WiFi	Provides information about Wireless Fidelity (WiFi) network capabilities available on the device, including: <ul style="list-style-type: none">• supported (yes, no)• status (on, off)• MAC address (for WiFi filtering purposes)• network name/access point

Windows schema

<i>Class</i>	<i>Property description</i>
BIOS (Basic Input/Output System; generally stored in a firmware chip located on the baseboard)	Provides information about the input/output activities at the client, including: <ul style="list-style-type: none"> • BIOS asset tag • patterns of textual information about BIOS data including scan date and size • baseboard revision level • copyright information • date • installation date • number of firmware revisions • identification in bytes • serial number for IDE disk • maker of the computer • monitor model and serial number • ROM family, size, and version • service tag • system model, name, and serial number • universal ROM
BOUND ADAPTER	Provides adapter information, including: <ul style="list-style-type: none"> • number of adapters • default gateway • description • whether DHCP is enabled (Dynamic Host Configuration Protocol: an Internet protocol for automating the configuration of computers that use TCP/IP) • DHCP server • IP address • when the adapter lease expires and when it was obtained • physical address • primary and secondary Windows Internet Net Server (WINS) • adapter status • subnet mask support
BUS (Broadcast and Unknown Server; data path on the computer's motherboard that interconnects the microprocessor with attachments to the motherboard in expansion slots such as hard disk drives, CD-ROM drives, and graphics adapters)	Provides information about the type of BUS present at the client, including: <ul style="list-style-type: none"> • EISA (Extended Industry Standard Architecture) slot number, product identification, and system board identification • NuBus board identification, name, and number (proprietary expansion bus used on Apple Macintosh personal computers) • PCI (Peripheral Component Interconnect) asset information, last BUS, and version information • type of BUS

<i>Class</i>	<i>Property description</i>
CACHE	<p>Provides information about the memory holding for recently accessed data, including:</p> <ul style="list-style-type: none"> • size • current type of SRAM (Static Random Access Memory) • whether the cache is enabled • method for correction of errors • FRU (field-replaceable units) group index • installed cache size • level • location • number • operational group index • designated socket (virtual connection between processes) and if a socket exists • supported type of SRAM • whether data is written to the main memory at the same time it's cached or only written to main memory when it's forced out of the cache
CDROM	<p>Provides information about the CD-ROM drive(s) including the letter and number of drives used at the client</p>
COMMUNICATIONS PORT	<p>Provides information about the port, including:</p> <ul style="list-style-type: none"> • address of the port • maximum speed at which the port allows transfer of data • name of the port • type of UART (Universal Asynchronous Receiver/Transmitter)
COMPUTER	<p>Provides information about the client computer, including:</p> <ul style="list-style-type: none"> • description • identification number and name • Client name • Client's domain name • Client user's full name • name of the Inventory server • last hardware and software scan dates and the date when the client last received an update by the Inventory server • Client user's login name • name of the domain controller • number of files on the computer • owner • type of inventory scan • type of computer

<i>Class</i>	<i>Property description</i>
COMPUTER MEMORY	<p>Provides memory information at the client, including:</p> <ul style="list-style-type: none"> • available and total conventional bytes • available and total extended bytes • status of memory cache • number of memory slots • available and maximum size of the pagefile (the reserved portion of a hard disk used as an extension of random access memory (RAM) for data that hasn't been used recently) • available and total physical bytes • physical size of the computer's heap (an area of pre-reserved computer memory that a program can use to store data in a variable amount that won't be known until the program runs) • available and total virtual bytes • status of the virtual memory
CONFIGURATION FILES	<p>Provides information for configuration files at the client including, autoexec.bat, config.sys, win.ini, and system.ini:</p> <ul style="list-style-type: none"> • data • date • path • size
COPROCESSOR	<p>Provides information about the client's computer processor, which assists the main processor by performing certain functions, including:</p> <ul style="list-style-type: none"> • Math (addition, subtraction and multiplication of integers) • PMMU (Paged Memory Management Unit: a hardware device or circuit that supports virtual memory and paging by translating virtual addresses into physical addresses)
CUSTOM DATA FOLDER	<p>Allows you to create one or more unique registry key name and value for the Windows client, which can then be included in custom views in Data views, Clients and Inventory.</p>
CUSTOM NAME VIEW	<p>Create the string or dword key name and value in the Custom Fields folder (which you must also create) under HKLM\SOFTWARE\Intel\Landesk\Inventory. You can create the key name and value via a Session Manager channel or manual entry.</p>
CUSTOM VALUE VIEW	<p>Create the string or dword key name and value in the Custom Fields folder (which you must also create) under HKLM\SOFTWARE\Intel\Landesk\Inventory. You can create the key name and value via a Session Manager channel or manual entry.</p>
DESK ACCESSORY DRIVER	<p>Provides name and version information about the installed desktop accessories at the client</p> <p>Provides information of the driver(s) installed at the client, including:</p> <ul style="list-style-type: none"> • address • name • unit number
DRIVERS AND SERVICES	<p>Provides information of the operating system driver(s)/service(s) installed at the client, including:</p> <ul style="list-style-type: none"> • address • name • status • unit number
ENVIRONMENT	<p>Provides a list of environment variable names, such as WINDIR and OS, and their corresponding values at the client, such as C:\WINNT or WINDOWS_NT</p>

<i>Class</i>	<i>Property description</i>
EXTENSIONS	Provides name and version information about installed files (via extensions) at the client
FILE SYSTEM DRIVER	Provides the name and status of the file system driver installed at the client
FIXED DRIVE	Provides information about the fixed file system at the client, including: <ul style="list-style-type: none"> • available storage space • number of bytes per sector (unless otherwise specified a sector of data consists of 512 bytes) • type of CMOS RAM (Complementary Metal Oxide Semiconductor: a semiconductor fabrication technology designed to achieve low power dissipation; Random Access Memory: the most common computer memory used by programs to perform necessary tasks while the computer is turned on) • cylinders • heads • number of fixed drive(s) • sectors • serial number of the drive(s) • total storage space available • description of the vendor of the drive(s)
FLOPPY DRIVE	Provides floppy drive(s) information at the client, including: <ul style="list-style-type: none"> • cylinders • heads • number of floppy drives • sectors • type of floppy drive(s)
FONTS	Provides name and version information about the fonts installed at the client
HANDHELD SYNC (PALM)	Provides information about the Palm device including: <ul style="list-style-type: none"> • last sync • modem port • serial port • sync path • sync version • USB supported
HANDHELD SYNC (WINDOWS CE)	Provides information about the device including: <ul style="list-style-type: none"> • device OEM info • device processor • device type • last sync • sync path • sync version
KERNEL DRIVER	Provides the name and status of the kernel driver (part of the operating system responsible for resource allocation, low-level hardware interfaces, security, etc.) installed at the client

<i>Class</i>	<i>Property description</i>
KEYBOARD	<p>Provides information about the keyboard used at the client, including:</p> <ul style="list-style-type: none">• code page (character set converter)• type of connector to the processor• time period between key stroke and character display• any extended information about the hardware• hardware identification number• number of function keys (special keys programmed to perform special actions)• type and sub type of hardware• rate at which a pressed key repeats itself, as in “keys repeating waaaay too faaaast”
LOGICAL DRIVE	<p>Provides information about the logical file system at the client, including:</p> <ul style="list-style-type: none">• available storage space• size allocated to the logical drive(s)• letter(s) representing logical drive(s)• number of files in the drive(s)• type of file system• number of folders in the drive(s)• date on which the drive(s) was created• date of last backup• whether the drive(s) is removable• unique address of the SCSI device (Small Computer System Interface: processor-independent standard, via a parallel bus, for system-level interfacing between a computer and intelligent devices like hard disks, floppy disks, CD-ROM, printers, scanners, etc.)• serial number• total storage space• type of logical drive(s)• name assigned to the drive(s)

<i>Class</i>	<i>Property description</i>
MEMORY SLOT	<p>Provides information about a plug-in memory board at the client, including:</p> <ul style="list-style-type: none"> grouped connections to the processor current sector interleave (mapping from logical to physical sector numbers on a magnetic disk designed to optimize sequential reads and writes) current speed current type whether the slot is bi-directional size of the slot that's enabled method for detecting errors and its capabilities installed size of the slot supported sector interleave maximum size of the module (RAM modules consist of several RAM chips mounted on a small circuit board) module's voltage number of slots number of errors in the memory slot operational group index how the slot is allocated supported connection speeds supported types of slots
MEMORYEMS (EMS: Expanded Memory Specification; memory paging scheme enabling access to memory other than conventional memory in real mode)	<p>Provides expanded memory information on the client, including:</p> <ul style="list-style-type: none"> available and total bytes of memory LIM EMS version address of the page (unit of transfer that moves infrequently-used parts of a program's working memory from RAM to a secondary storage medium, usually disk, frame, or packet)
MEMORYXMS (XMS: Extended Memory Specification; requirement describing extended memory in real mode for storing data, rather than executable code)	<p>Provides extended memory information on the client, including:</p> <ul style="list-style-type: none"> address line of the A20 handler (memory manager software controlling access to the HMA: High Memory Area, the first 64 kilobytes minus 16 byte of the extended memory) available and total bytes of memory driver version HMA (High Memory Area), as well as the available HMA largest available unit of data or memory version of the XMS (Extended Memory Specification)

<i>Class</i>	<i>Property description</i>
MODEM	<p>Provides information about a modem at the client, including:</p> <ul style="list-style-type: none">• baud rate (the unit in which the information carrying capacity of a communication channel is measured; one baud is one symbol—state-transition or level-transition—per second)• number of character bits (9 bits equal 1 byte; 1 byte equals 1 character)• flow control (the collection of techniques used in serial communications to stop the sender from sending data until the receiver can accept it)• maker of the modem• model• number• parity (an extra bit added to a byte or word to reveal errors in storage)• port• stop bits (normally a byte or character, extra “1” bits that follow the data and any parity bit that mark the end of a unit of transmission)
MOTHERBOARD	<p>Provides information about the main circuit board installed at the client, which contains the BUS; microprocessor; and integrated circuits used for controlling built-in peripherals, such as the keyboard, text and graphics display, serial ports and parallel ports, joystick, and mouse interfaces, including:</p> <ul style="list-style-type: none">• chipset (collection of integrated circuits designed to be used together for some specific purpose)• maker of the motherboard• name of product• serial number• product version
MOUNT	<p>Provides information about the mount (which makes a file system available for access by attaching a named file system to the file system hierarchy at the pathname location directory) at the client, including:</p> <ul style="list-style-type: none">• storage available• device name• file system• directory of mount• total storage
MOUSE	<p>Provides information about the installed mouse at the client, including:</p> <ul style="list-style-type: none">• number of buttons• type of connector• name and version of driver• line on which the computer stores information to identify the source of the interrupt• type of mouse

<i>Class</i>	<i>Property description</i>
NETBIOS (Network Basic Input/Output System; set of network commands that the application program issues in order to transmit and receive data to another host on the network)	Provides information about the NetBIOS at the client, including: <ul style="list-style-type: none"> • whether NetBIOS exists • current maximum network control blocks (NCBs) on the LAN • current maximum pending sessions on the LAN • available circuit mode data blocks on the LAN • maximum hardware circuit mode data blocks on the LAN • maximum hardware session count on the LAN • local session count on the LAN • maximum size of packet on the LAN • name and number of the LAN • name of the table count on the LAN • pending session count on the LAN • software version on the LAN • number successful receipts and transmissions of data
NETWARE INFO	Provides information about Novell, Inc.'s proprietary networking operating system at the client, including: <ul style="list-style-type: none"> • accounting version • major and minor version of the C library, as well as the revision number • whether there is internet bridge support, and maximum connections and volumes supported • NetWare revision level, as well as version and sub version • peak connections used • version of the print server used • version of queuing • security restriction level • level of system fault tolerance (SFT) • level of transaction tracking system (TTS) • version of the value added process (VAP) • version of the virtual console
NETWORK	Provides information about the network connection type at the client, including: <ul style="list-style-type: none"> • version and name of AppleTalk (proprietary LAN protocol for communication between Apple products like Macintosh and other computers) • address, network number, node address and version of IPX (Internetwork Packet eXchange: network layer protocol in Novell NetWare file server operating system) • NIC address • driver description, driver version, operating system text and version of Shell (Unix command interpreter used to pass commands to an operating system) • version of SPX (filename extension for Screen Peace eXtension files) • TCP/IP (Transmission Control Protocol over Internet Protocol) address and host name • whether IP routing is enabled
NETWORK (cont.)	<ul style="list-style-type: none"> • whether the TCP/IP NetBIOS resolution uses DNS (Domain Name System: general-purpose distributed, replicated, data query service chiefly used on Internet for translating hostnames into Internet addresses) • whether the TCP/IP WINS proxy is enabled (Windows Internet Naming Service: resolves NetBIOS names to IP addresses) • type of network

<i>Class</i>	<i>Property description</i>
NETWORK ADAPTERS	Provides information about devices that make different pieces of apparatus compatible at the client, including: <ul style="list-style-type: none"> connector type rate at which data is moved description number physical address vendor
ODBC SYSTEM DSN (Open Database Connectivity system that stores your database connection information in the system registry of the Web server)	Provides information about ODBC file system including: <ul style="list-style-type: none"> name driver description database server
OS	Provides information about the operating system at the client, including: <ul style="list-style-type: none"> name version Windows OS version
PORTS	Provides information about ports—logical channel or channel endpoint in a communications system—at the client, including the serial interface controller and interface adapters
PRINTER	Provides information about the installed printer(s) at the client, including: <ul style="list-style-type: none"> type of data used by the printer default printer driver name number port used by the printer printer's processor
PRINTER PORT	Provides information about the installed printer's port at the client, including the name and address

<i>Class</i>	<i>Property description</i>
PROCESSOR	<p>Provides information about the processor at the client, including:</p> <ul style="list-style-type: none"> • features for cellular multiprocessing instructions (processors separated into computing environments running different operating systems) • conditional move instructions • identification • computer checks for exceptions and architecture • range of the memory type • MMX technology (Matrix Math eXtensions: set of 57 extra instructions built into some versions of Intel's Pentium microprocessors) • model any model-specific registers • whether APIC (Advanced Programmable Interrupt Controller) is on the processor • whether the global page is enabled • whether any extensions to page size are available
PROCESSOR (cont.)	<ul style="list-style-type: none"> • physical address extension • processor count and serial number • whether the processor accepts a signature • speed • stepping • time stamp counter • processor type • vendor • any virtual mode extensions
RESOLUTION	<p>Provides information about resolution at the client, including:</p> <ul style="list-style-type: none"> • colors available and the number • frequency and method of refresh • maximum number of pixels (number of horizontal pixels x number of vertical pixels) that display
RESOURCE	<p>Provides information about various hardware resources and the devices that use them, including:</p> <ul style="list-style-type: none"> • channel and port of the DMA (Direct Memory Access: a facility of some architectures that allows a peripheral to read and write memory without intervention by the CPU) • IRQ (Interrupt ReQuest: the name of an input found on many processors that causes it to suspend normal instruction execution temporarily and start executing an interrupt handler routine) • memory • name • port

Class	Property description
SCSI DEVICE (Small Computer System Interface; processor-independent standard, via a parallel bus, for system-level interfacing between a computer and intelligent devices like hard disks, floppy disks, CD-ROM, printers, scanners, etc.)	Provides information about the SCSI device at the client, including: <ul style="list-style-type: none"> • controller • device type • model name and number • revision level • name of the vendor
SERVICE	Provides information about service(s) at the client, including the name and status
SOFTWARE	Provides information about the package file—written programs, procedures, or rules and associated documentation pertaining to the operation of a computer system and that are stored in read/write memory—at the client, including: <ul style="list-style-type: none"> • whether attributes are hidden, read only, and/or system • file date • file permission mask (the ability to access, read, write, execute, traverse, etc. a file or directory) • file size • date a software application was last accessed by the user <p>Note: Last Accessed Date is only available for Windows clients views through the Data views, Inventory and Clients links. It is used to calculate the License compliance schema properties that represent the number of licenses not accessed in 30, 60, and 180 days. To view a report that associates corporate software applications with client users, run the Client Usage Detail report in Home, Reports, License Compliance.</p> <p>Note: Last Accessed Date is only accurate to the day for FAT and FAT32 systems. Time will be accurate for NTFS systems.</p> <ul style="list-style-type: none"> • name • path • file version
SOUND CARD	Provides information about the sound card at the client, including: <ul style="list-style-type: none"> • DMA (Direct Memory Access: a facility of some architectures that allows a peripheral to read and write memory without intervention by the CPU) • IRQ (Interrupt ReQuest: name of an input found on many processors that causes it to suspend normal instruction execution temporarily and start executing an interrupt handler routine) • maker of the sound card • type • version
SYSTEM	Provides information about the client computer, including: <ul style="list-style-type: none"> • asset tag • type of chassis (metal mounting for the circuit components) • manufacturer • model • serial number

<i>Class</i>	<i>Property description</i>
SYSTEM SLOT	<p>Provides information about the client computer slot, including:</p> <ul style="list-style-type: none"> • description • allocation • identification • length • number of slots • type • usage • width
USB CONTROLLER	<p>Provides information about the USB controller including:</p> <ul style="list-style-type: none"> • controller number • name • manufacturer
USB DEVICE	<p>Provides information about the USB device including:</p> <ul style="list-style-type: none"> • device number • name • manufacturer
VIDEO	<p>Provides information about the video card at the client, including:</p> <ul style="list-style-type: none"> • BIOS version • colors available • driver date • name • version • frequency of refresh • date of release • how it's mapped to the client's memory • resolution
VIDEOADAPTER	<p>Provides information about the video card adapter at the client, including:</p> <ul style="list-style-type: none"> • adapter string • chip type • color device • type of DAC (Digital to Analog Converter: a device that takes a digital value and outputs a voltage proportional to the input value) • horizontal DPI (dots per inch) • main monitor • memory • number • type • vertical DPI • manufacturer name, support, and version of the VESA (Video Electronics Standards Association: an industry standards organization that created the 800 x 600 pixel Super VGA (SVGA) display and its software interface)

<i>Class</i>	<i>Property description</i>
VOLUME	Provides information about the volume—a special file on a disk/directory that contains a list of all the ordinary files on the disk and their addresses—at the client, including: <ul style="list-style-type: none"> • number of blocks available • directory slots available • number of directory slots • name • number of sectors per block • total number of blocks • type
XBIOS (Extended Basic Input/ Output System)	Provides information about the extended BIOS at the client, including asset information and service tag

Server schema

The server schema includes access to client group, log data, and software package tracking classes/properties.

<i>Class</i>	<i>Property description</i>
Client	Provide information about the clients defined on your system, including: <ul style="list-style-type: none"> • Afaria Device ID • Afaria Device ID naming option used to create the Afaria Device ID value, defined as follows: <ul style="list-style-type: none"> • 0 – User Name • 1 – IMEI Number • 2 – IMSI Number • 3 – Telephone Number • 4 – Device Serial Number • 5 – Device Sync Name • 6 – IP Address • 7 – Value Specified by Registry Value • 8 – Value Specified by Database Value • 9 – OS Platform • client type • code signer for Windows Mobile clients • first connection time • last connection time • name, as per the ClientMachineName session variable • OS shell for handheld clients, as per the ClientOsShell session variable • OS version for handheld clients, as per the ClientOsVersion session variable

<i>Class</i>	<i>Property description</i>
Client Group	Provides information about the client groups defined on your system, including: <ul style="list-style-type: none">• client group member• description of the group• last time the group was updated• group name• group type, as dynamic or static
File Transfer Log	Provides information about files transferred through the system, including: <ul style="list-style-type: none">• number of bytes sent• name of the client in the session• path at the client where the file was sent/received• command• time the file transfer ended• name of the channel or channel set the client requested• name of the server sending/receiving the file• path at the server where the file was sent/received• file size• time the file transfer started• status of the file transfer
Message Log	Provides messages specific to the server, including: <ul style="list-style-type: none">• date and time the message was sent• error• message• display name of the server• name of the server• name of the server user• type of message

Class	Property description
Package Tracking	<p>Provides status information about Software Manager channels, including:</p> <ul style="list-style-type: none"> • Cleanup, which represents that a Windows client channel was delivered to the client and not installed from a LAN location <ul style="list-style-type: none"> —numeric indication of the success/failure regarding the cleanup —date on which cleanup occurred —version of the channel at the time of cleanup —readable indication of the state of the cleanup • Delivery Completed, which represents that data is updated every time the channel is delivered to the client (unavailable on LAN based channels) <ul style="list-style-type: none"> —numeric indication of the success/failure regarding content delivery —date on which channel content was delivered —version of the channel at the time content was delivered —readable indication of the state of content delivery • Delivery Started, which represents that channel delivery has started <ul style="list-style-type: none"> —date on which channel delivery started at the client —version of the channel when delivery of the channel started • Install Completed, which represents completion of channel installation at the Windows client; and after channel delivery on channels for handheld clients <ul style="list-style-type: none"> —numeric indication of the success/failure —date channel installation completed; channel delivery —version of the channel when installation completed; channel delivery —readable indication of the state channel installation; channel delivery • Install Started, which represents that channel installation has progressed as far as the setup executable on Windows client channels; and after channel delivery on channels for handheld clients <ul style="list-style-type: none"> —numeric indication of the success/failure —date channel installation started; channel delivery —version of the channel when installation started; channel delivery —readable indication of the state channel started; channel delivery • LAN Based indicates that the Windows client channel was installed from a LAN location • Last Published Date indicates the last date the channel was published • Most Recent Action indicates the last thing that happened to the channel <ul style="list-style-type: none"> —numeric indication of the success/failure of the last action —date on which the last action occurred —version of the channel at the time the last action occurred —readable indication of the state of the last action • Name of the channel • Package Path indicates the path of the source files for the software channel • Setup Based indicates whether the Windows client channel contains a setup executable file • Setup Executable Extension indicates the type of setup executable file • Significant Version indicates the channel version when an action occurred • Uninstall, which represents that the channel was uninstalled at the client <ul style="list-style-type: none"> —numeric indication of the success/failure of the uninstall —date on which the uninstall occurred —version of the channel at the time the uninstall occurred —readable indication of the state of the uninstall

License compliance schema

The License compliance schema resides under the server node but is only available through License compliance view. It includes the following properties.

Property description

Number of software licenses installed

Number of software licenses purchased

Percentage of software licenses installed relative to the number purchased

Number of licenses not accessed in 180 days

Number of licenses not accessed in 30 days

Number of licenses not accessed in 60 days

Software application name

Client category for which software was purchased, for example Palm handheld software

Effective date of software license

Expiration date of software license

Manufacturer of software

Notes about the software license

Size of software

Version of software

Creating Custom Database Views

Create custom database views to return data from the database that is not already represented in a predefined view.

The View editor—which you can access through Data views, Clients, Logs, Inventory, and License compliance—allows you to create custom views (queries) of inventory, log, and server-related data.

After you label your custom view with a name and description, you click the Add column link to open the Add column dialog box. It's through this dialog box that you have access to the database schemas, classes, and properties.

The Add column dialog box displays schemas specific to Clients, Logs, and Inventory views. For example, Logs view displays only log data. The dialog box at right is found in Clients view.

Creating a custom view for the different product views follows the same general procedure, but each with access to a particular set of database schemas, classes, and properties.


The View editor dialog box is titled "View editor" and contains the following sections:

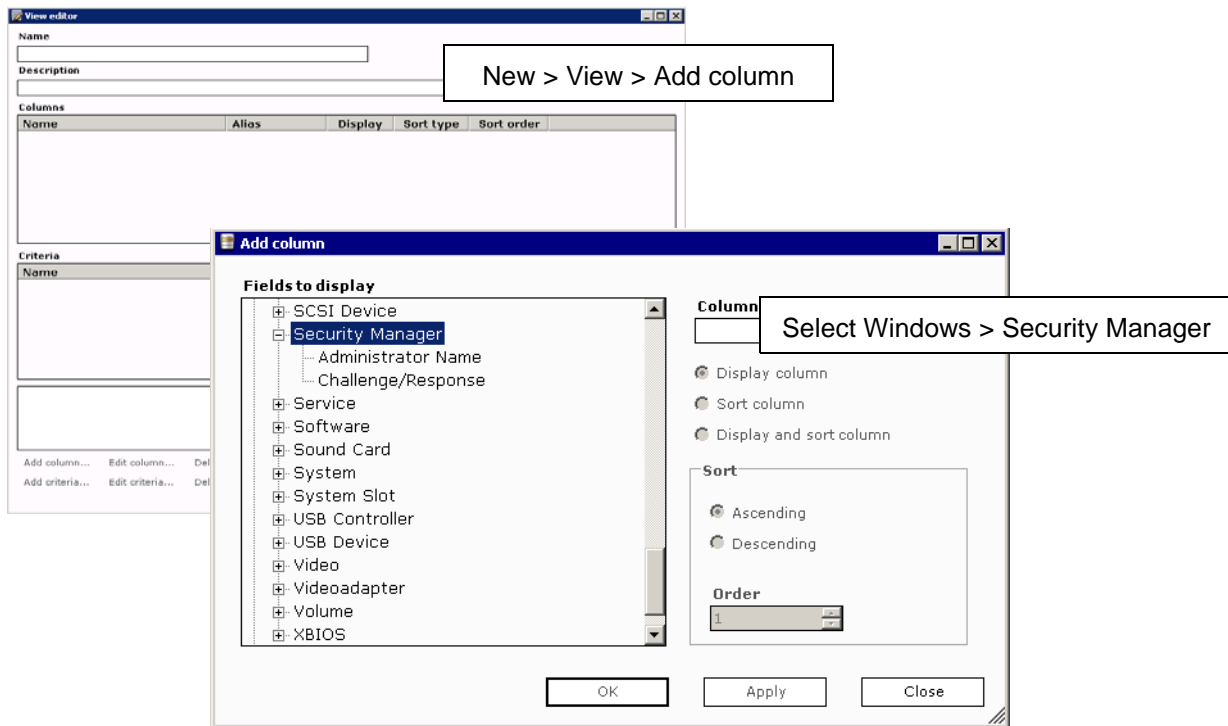
- Name:** A text input field.
- Description:** A text input field.
- Columns:** A table with columns: Name, Alias, Display, Sort type, Sort order.
- Criteria:** A table with columns: Name, Operator, Value, Condition.
- Buttons:** Add column..., Edit column..., Delete column, Move up, Move down, Add criteria..., Edit criteria..., Delete criteria, Group, Ungroup, Display SQL statement..., OK, Cancel.

The Add column dialog box is titled "Add column" and contains the following sections:

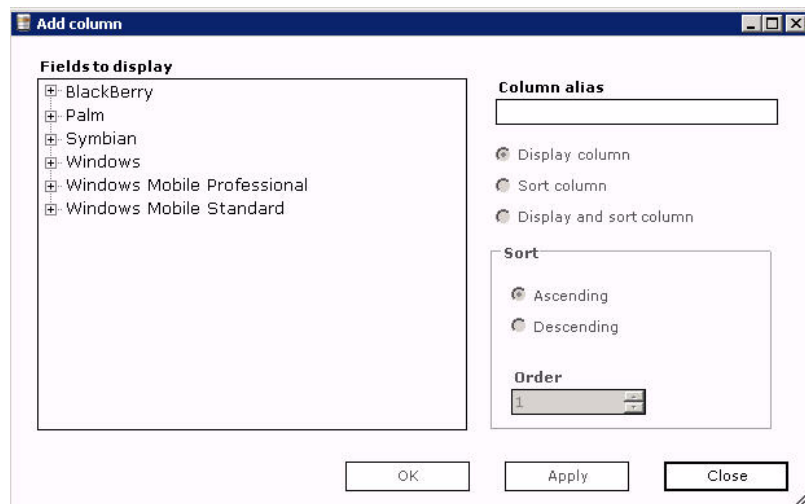
- Fields to display:** A list box containing BlackBerry, Palm, Symbian, Windows, Windows Mobile Professional, and Windows Mobile Standard.
- Column alias:** A text input field.
- Display options:** Radio buttons for Display column, Sort column, and Display and sort column.
- Sort:** Radio buttons for Ascending and Descending.
- Order:** A text input field with the value "1".
- Buttons:** OK, Apply, Close.

Creating a Custom Data View Example – Custom Client Data View

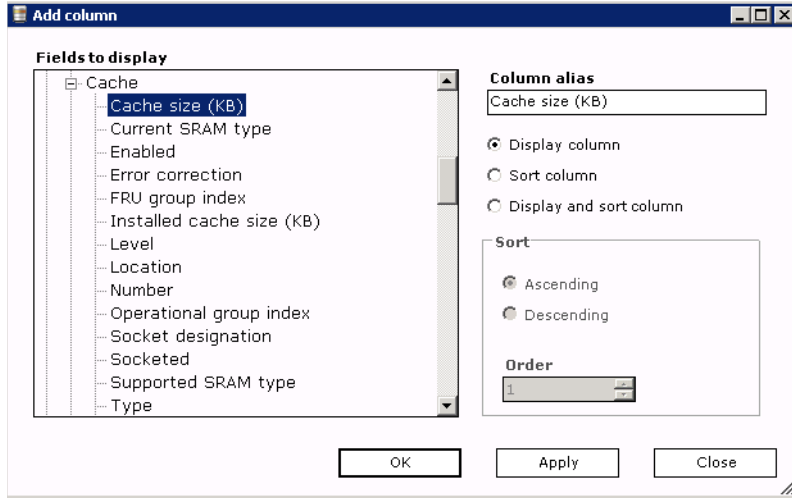
To create a new client view, select the top node in the clients tree and click  **New**, then select **View**. The View editor dialog box appears. Use it to label and create/manage columns in the view.



The Fields to display list contains the schemas available to you for the clients in the Clients view. Most are client inventory specific; Server includes tables specific to software package tracking, groups of clients, file transfer log data, and message log data.



Each schema class contains properties of data from which you can create custom views. Notice the expanded Windows class in the dialog box below.



Select a property in the Fields to display list. The column's "common" name in the **Column alias** field. You can save the column under a different name for sorting purposes.

By default, each column you select displays in the view, but you can hide a column by clearing the **Display column** check box.

Select the **Sort column** check box to enable the Sort group box. A sort automatically queries information in **Ascending** (default) order unless you select **Descending**. The first column that you elect to sort defaults to **Order "1,"** but you can alter the sort order by entering a value or using the spin buttons.

To display and sort the column, select **Display and sort column** and then follow the sort instructions above.

Click **OK** to save the new column to the Columns list in the View editor dialog box. The Add column dialog box closes.

Click **Apply** to save the new column to the Columns list but keep the Add column dialog box open so that you can continue creating columns. When finished, click **Close**.

Click **Close** to return to the View editor dialog box without saving changes.

The Columns list in the View editor dialog box displays the data to be collected by your view.

To alter the details of an existing column in the view, select it and then click **Edit column**. The Edit column dialog box appears with the schemas collapsed.

To remove a column from the view, select it and then click **Delete column**.

To change the order of columns, select the column to move and then click **Move up** or **Move down**.

To add criteria to a column, click **Add criteria**. In the Add criteria dialog box, select the column from the Fields to display list, then choose an operator from the **Operator** drop-down list.



The operators available depend upon the property you select. Choices can include =, !=, <, >, >=, <=, or Like.

Value defaults to Custom, which allows you to enter a value in the field. You can also select From database and then choose a value from the drop-down list.

Set the **Condition**.

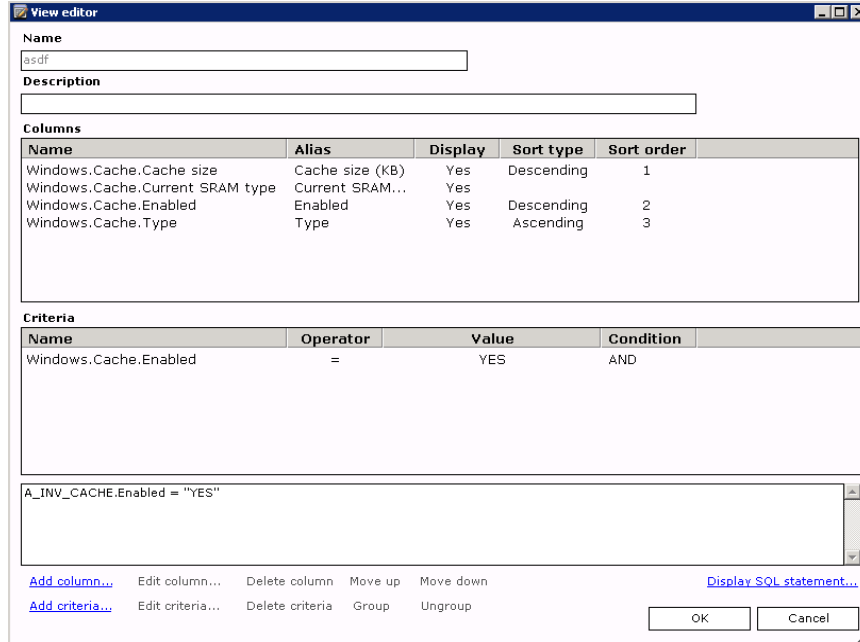
Click **OK** to save the column criteria to the Criteria list in the View editor dialog box. The Add criteria dialog box closes.

Click **Apply** to save the column criteria, but keep the Add criteria dialog box open to continue defining column criteria. When finished, click **Close**.

Click **Close** to return to the View editor dialog box without saving changes.

Name	Alias	Display	Sort type	Sort order
Windows.Cache.Cache size	Cache size (KB)	Yes	Descending	1
Windows.Cache.Current SRAM type	Current SRAM...	Yes		
Windows.Cache.Enabled	Enabled	Yes	Descending	2
Windows.Cache.Type	Type	Yes	Ascending	3

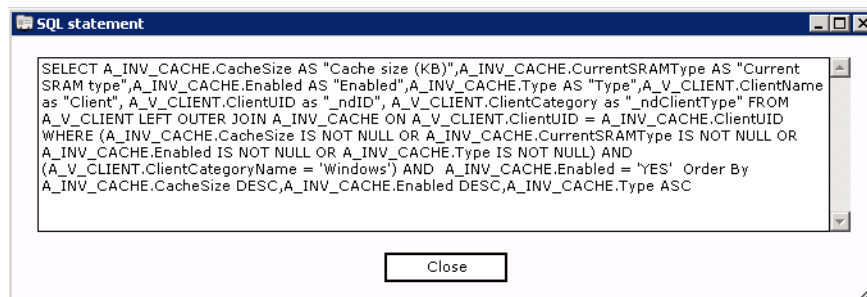
Your column criteria displays in the Criteria list. To alter a column's criteria, select it and then click **Edit criteria**. The Edit criteria dialog box appears at the property specified with criteria.



Viewing a Custom View's SQL Statement

View a custom view's SQL statement to review the statement or copy it to the Windows clipboard for subsequent pasting.

To view a custom view's SQL statement, open the view's view editor and click **Display SQL Statement**. The SQL statement dialog box appears. To copy the statement to the Windows clipboard for other use, right-click the statement and on the shortcut menu choose **Select All**, then **Copy**. Paste the statement into an editor of your choice.



Click **Close** to return to the View editor dialog box.

To save the view and return to Clients view, click **OK**.

The new view displays in the left pane of Clients view. When selected, your column attributes, including client name, display in the right pane and the view runs. The complexity of the view and the database size determine the time required to display results.

To alter the attributes of a custom view, right-click the view and then choose **Edit** on the shortcut menu. Use the View editor dialog box to make alterations.

Custom Views and Your Multitenancy Environment

Support – Multitenancy

The multitenancy database design has implications for custom views. The system attempts to filter custom results by tenant by modifying the associated SQL script at runtime. However, it may not always be successful. Therefore, test your custom items after accumulating data for multiple tenants to evaluate how they are performing and understand whether the data returned is filtered by tenant.

Custom items produce one of the following results:

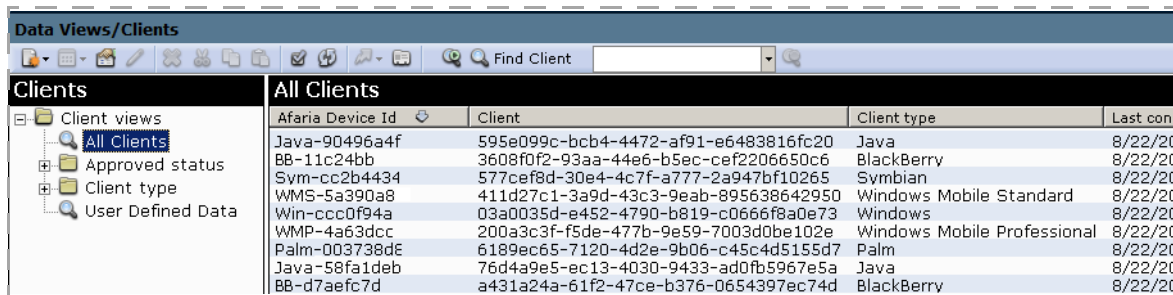
- error-free results that are filtered by tenant
- error-free results that are not filtered by tenant
- fatal errors during execution

You may need to delete damaged items and re-create them with modifications. Generally, adding a tenant-specific property allows the system to filter by tenant.

Custom items that you create are available to all tenants, rather than only for the originating tenant.

Managing Client Data

The Data Views Clients view presents data from a client perspective rather than from a component perspective. You can examine client data and take some actions on clients without leaving the view. You can also create folders, views, groups, and SQL views to collect client data.



Data Views/clients				
Clients				
All Clients				
Afaria Device Id	Client	Client type	Last con	
Java-90496a4f	595e099c-bcb4-4472-af91-e6483816fc20	Java	8/22/20	
BB-11c24bb	3608f0f2-93aa-44e6-b5ec-cef2206650c6	BlackBerry	8/22/20	
Sym-cc2b4434	577cef8d-30e4-4c7f-a777-2a947bf10265	Symbian	8/22/20	
WMS-5a390a8	411d27c1-3a9d-43c3-9eab-895638642950	Windows Mobile Standard	8/22/20	
Win-ccc0f94a	03a0035d-e452-4790-b819-c0666f8a0e73	Windows	8/22/20	
WMP-4a63dcc	200a3c3f-f5de-477b-9e59-7003d0be102e	Windows Mobile Professional	8/22/20	
Palm-003738dE	6189ec65-7120-4d2e-9b06-c45c4d5155d7	Palm	8/22/20	
Java-58fa1deb	76d4a9e5-ec13-4030-9433-ad0fb5967e5a	Java	8/22/20	
BB-d7aefc7d	a431a24a-61f2-47ce-b376-0654397ec74d	BlackBerry	8/22/20	

Clients view contains two panes:

- The left pane displays available folders and views. You can define your own or use the predefined views. Each view item in the pane has a shortcut menu.



The User Defined Data view displays the fields you create. For information about creating user defined fields, see [“User defined fields” on page 159](#).

- The right pane displays client data that is specific to the item selected in the left pane. Each client row has a shortcut menu.

The following right-pane shortcut tasks relate to the clients:

- [“Searching for a Client” on page 397](#)
- [“Revoking and Approving Clients” on page 399](#)
- [“Opening Client Mini-views” on page 401](#)
- [“Viewing Client Properties” on page 409](#)
- [“Changing a Client’s Tenant Association” on page 410](#)
- [“Changing a Device ID” on page 411](#)
- [“Deleting Client Data” on page 412](#)
- [“Combining a Client’s Afaria Client ID” on page 413](#)
- [“Managing Client Outbound Notification Addresses” on page 416](#)
- [“Sending an Outbound Notification to Run a Channel” on page 417](#)
- [“Sending an Outbound Notification to Apply Policies” on page 418](#)

- [“Sending BlackBerry Security Commands” on page 421](#)
- [“Wiping a Remote Device” on page 422](#)
- [“Recovering a Data Security Manager Client Password” on page 425](#)
- [“Managing Data Security Manager Administrator Accounts” on page 431](#)

See also:

- [“About Outbound Notifications” on page 415](#)
- [“Managing Client Outbound Notification Addresses” on page 416](#)
- [“Client Notifications Status” on page 419](#)

The following left-pane shortcut tasks relate to the folders and views:

- [“Creating a New Client Folder” on page 432](#)
- [“Creating a Custom Client View” on page 432](#)
- [“Renaming a Folder or View” on page 432](#)
- [“Viewing Folder or View Properties” on page 433](#)
- [“Creating a Group Within a View” on page 434](#)
- [“Creating a New SQL View Within a View” on page 438](#)

Searching for a Client

The product provides features for searching for clients on the Data Views pages.

- Simple search:
 - Available on all views.
 - Search scope includes all the clients in the current view.
 - Search criteria is evaluated against the client name field.
- Advanced search:
 - Available only on the All Clients view.
 - (Non-multitenancy) Search scope includes the user-selected list of client types.
 - (Multitenancy) Search scope includes the user-selected list of tenants and client types.
 - Search criteria is evaluated against multiple, user-selected fields including client name, Afaria device ID, telephone number, and additional fields.

Performing a Simple Client Search

- 1 Define the search scope by selecting any Data Views Clients view.
- 2 Define the search criteria by typing a complete or partial client name in the **Find Client** search box on the toolbar, using literal, or literal plus wildcard, characters. The search supports wildcard characters "*" and "?" for multiple characters and single characters, respectively.
- 3 Click **Find Client** to return results to the page.

The results include the clients matching the criteria up to the number of result rows defined by the Options dialog, also located on the toolbar.
- 4 (Optional) To view more matching results, increase the number of rows in the Options dialog and re-run the search.

The search criteria remains in the **Find Client** search box until you click the **Cancel Search and Find** icon.

Performing an Advanced Client Search

- 1 Open the Data Views All Clients view.
- 2 Click the Advanced Client Search icon.
- 3 (Multitenancy only) Define the tenant search scope by selecting tenants.

Only tenants that are enabled and assigned to your user role appear in the available tenants list.
- 4 Define the client type scope by selecting the client types.
- 5 Select the search fields to query against the search criteria.

- 6 (Optional) Define the search criteria by typing a string in the **Search Value** box. Leaving the box empty is interpreted as *all values*.

The string represents any part of the search field. Wildcard characters are not supported as search criteria, they are interpreted literally.

- 7 Click **Search** to return results to the search dialog's Clients Found list.

The search process returns records that include the search criteria string in any part of the search fields. For example, criteria "543" returns a record with a search field value "ID_54359".

- 8 (Optional) Redefine your scope and criteria and re-run the search until the search results meet your needs.

- 9 In the Clients Found list, select an individual client or a node that contains the clients you want to view and click **OK** to populate the Data Views All Clients page with the results.

The tenant context changes according to your selection.

The search criteria results remain on the Data Views All Clients page until you click the **Cancel Search and Find** icon.

Revoking and Approving Clients

Clients may be manually approved or revoked by the Afaria administrator. Approved clients can run sessions and request channels. Use the Approved status folder in Data Views, Clients to revoke or approve clients.

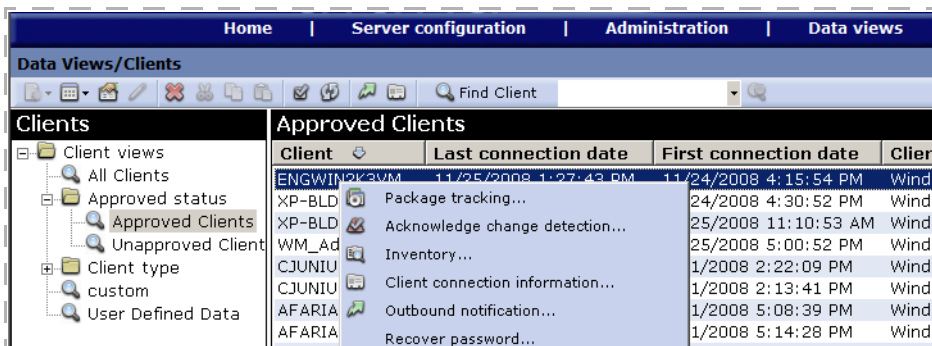


Revoking Client Approval

Use the revoke client approval feature to remove the ability for the client to run sessions.

To revoke a client approval:

- 1 Select **Approved Clients** from the Approved status folder.
- 2 Right-click on a client from the Approved Clients list and choose **Revoke Client**.



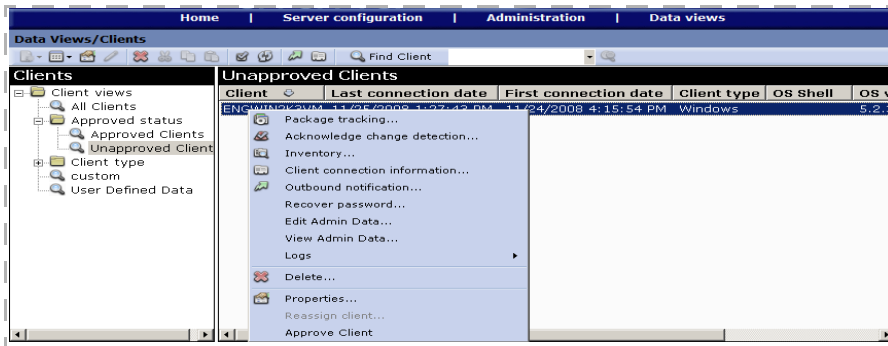
The client name is removed from the approved list and listed as an unapproved client in the Approved status folder.

Approving a Client

Use the approve clients feature to provide the ability for the client to run sessions during the next connection to the Afaria Server.

To approve a client:

- 1 Select **Unapproved Clients** from the Approved status folder.
- 2 Right-click on a client from the Unapproved Clients list in the right pane and select **Approve Client**.



The client name is removed from the list and listed as an approved client in the Approved status folder.

Opening Client Mini-views

Through Clients view, you can open views of client information that you would otherwise find in Logs, Inventory, and Package tracking views. You can open the same mini-views for several clients and/or different mini-views for the same client and keep them all open at the same time without leaving Clients view.

To open a client mini-view, select the left-pane view that contains the client with data you want to view. In the right pane, right-click the client, then choose the appropriate view. The product supports the following mini-views:

- Package tracking – tracking the status of Software Manager channels
- Acknowledge change detection – detected inventory changes
- Inventory – Client hardware and software inventory including directory scan data and configuration files for Windows clients
- Logs – logs for file transfers and sessions logs

Package Tracking Example

The following window is an example of the Package tracking view for a selected client. Information that displays in this view includes the Software Manager channel and channel path; number of channel modifications; delivery/installation status at the client; whether the Windows client user performed a cleanup after installation; time/date of channel installation; channel state; delivery model; date on which the channel was last published; and client type for the channel.



For more information on Package tracking view, see [“Track Software Manager channels” on page 467](#).

You can update the software channel’s status at the client by clicking  **Refresh**.

To view the properties of the package, click  **Package properties** on the button bar. The read-only Software package properties dialog box appears. Use it to view the name and characteristics of the selected channel.



For more information on the Software package properties dialog box, see [“View package properties” on page 468](#).

Software package	Channel path	Description	Modification number	Status
SWMgr	\\AFARIAW2K3R2		3	Delivery completed

Property	Value
Channel path	\\AFARIAW2K3R2
Channel state	Published
Delivery model	Delivery based
Description	
Modification number	3
Package Client type	All Windows Clients
Published date	12/1/2008 5:13:06 PM
Server	AFARIAW2K3R2
Setup executable extension	
Type	Non-Setup based

To find information on a specific software channel, enter the string data in the field provided and then click **Find package**.

Acknowledge Change Detection Example

The following window is an example of the Acknowledge changes detection view for a selected client. Information that displays in this view includes the type of client (schema); class; property

monitored for changes; previous value of the property and new value; and date/time of the inventory change.



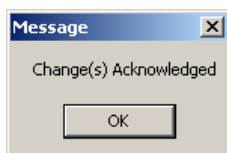
For more information on configuring inventory changes to monitor, see ["Monitoring Inventory Changes"](#) on page 453.

Client	Class	Property	Previous value	New value	Date/Time
AFARIAW2K3R2	Computer	Last hardw...	12/11/2008 12...	12/11/2008 12...	12/11/2008 12:25:01 ...
AFARIAW2K3R2	Computer	Last hardw...	12/11/2008 12...	12/11/2008 12...	12/11/2008 12:22:01 ...

Current view: Acknowledge changes for Client: AFARIAW2K3R2 (2 Row(s))

You can update the data displayed by clicking **Refresh**.

To acknowledge that you've seen a client's inventory changes click **Acknowledge Change Detection** on the button bar.



In the Message box, click **OK** to acknowledge the client's changes. The selected row is removed from the view.

Client Inventory Example

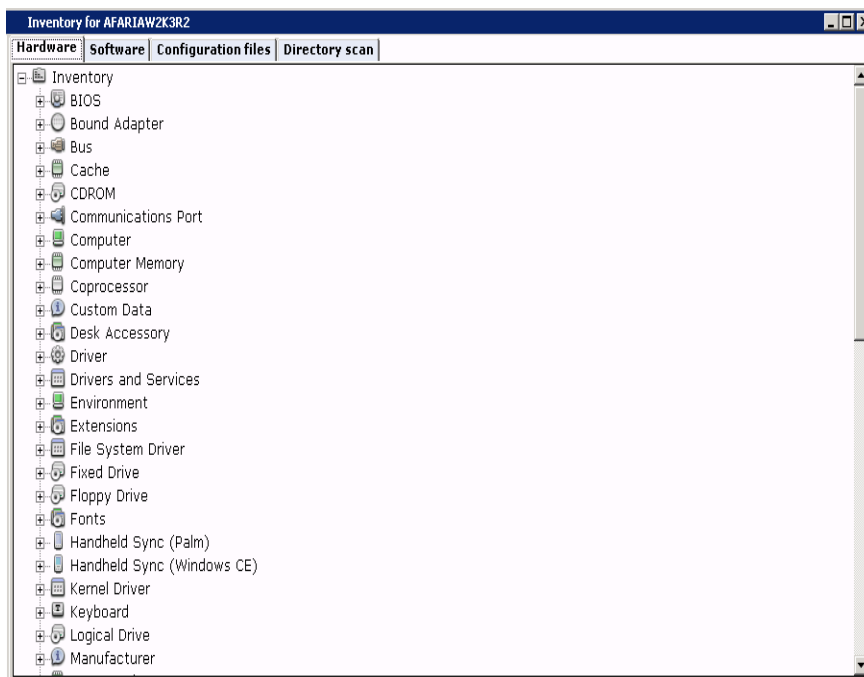
The following window is an example of the client inventory view for a selected client. All four property pages are available for Windows clients. Hardware and Software are available for handheld clients:

- **Hardware** lists the hardware data that Inventory Manager collected and reported for the selected client. The data collected includes all of the classes and properties specific to the client type.



- **Software** lists the software data that Inventory Manager collected and reported for the selected client. The data collected includes all of the classes and properties specific to the client type.
- **Configuration files** displays the name of the configuration file; size of the file in bytes; time at which the file was last modified on the Windows client; when the file was reported to the database; and contents of the selected configuration file.
- **Directory scan** displays information on the directory and file structure of all local hard drives at the Windows client if you defined the Inventory Manager channel to collect this data. Information reported includes:
 - File size in bytes
 - File creation date
 - Last date and time file was modified
 - Last date and time file was accessed
 - Last date and time file was accessed



For more information on the client inventory property pages, see [“Viewing a Specific Client’s Inventory Data”](#) on page 463.



Logs Examples

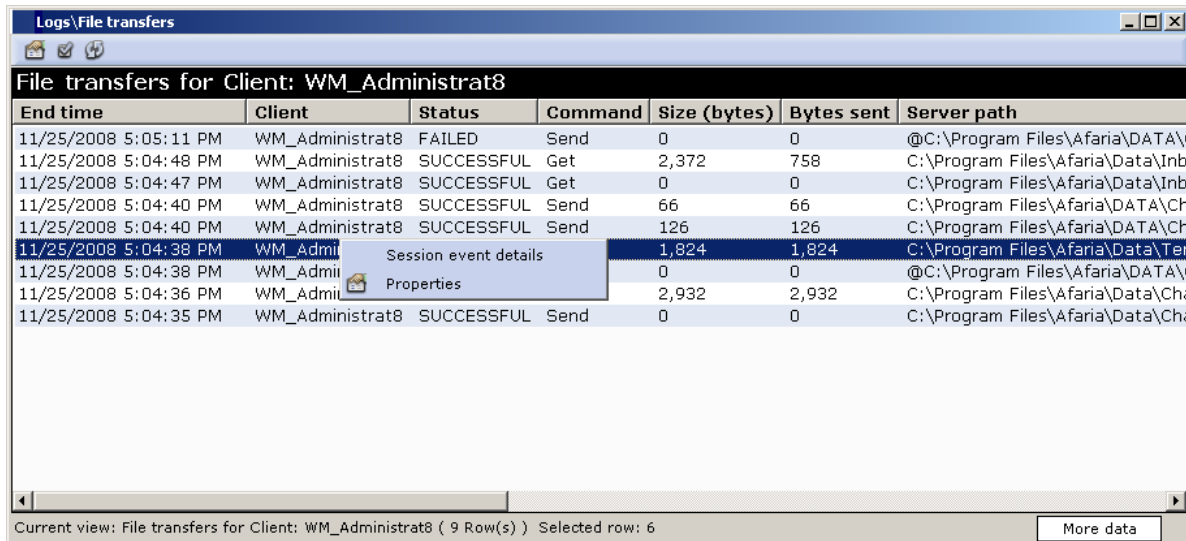
The following windows are examples of the Logs, File transfers and Sessions views for a selected client. In each view, to change the number of data rows retrieved, click  **Options**; enter the new value, then click **OK**. To display more rows without changing the options, click **More data** at the lower-right of the view. To update data, click  **Refresh**.



For more information on working with log views, see [“Working with Logged Actions”](#) on page 439.

File Transfers

Information that displays in this view includes the session end time; name of the client; status of the transfer; Session Manager event (Command); size of the file; bytes/kilobytes sent (Windows clients/handheld clients); path at the server to the source of the file; destination path at the client; and the name of the server providing the channel/channel set.



End time	Client	Status	Command	Size (bytes)	Bytes sent	Server path
11/25/2008 5:05:11 PM	WM_Administrat8	FAILED	Send	0	0	@C:\Program Files\Afaria\DATA\
11/25/2008 5:04:48 PM	WM_Administrat8	SUCCESSFUL	Get	2,372	758	C:\Program Files\Afaria\Data\Inb
11/25/2008 5:04:47 PM	WM_Administrat8	SUCCESSFUL	Get	0	0	C:\Program Files\Afaria\Data\Inb
11/25/2008 5:04:40 PM	WM_Administrat8	SUCCESSFUL	Send	66	66	C:\Program Files\Afaria\DATA\CH
11/25/2008 5:04:40 PM	WM_Administrat8	SUCCESSFUL	Send	126	126	C:\Program Files\Afaria\DATA\CH
11/25/2008 5:04:38 PM	WM_Administrat8	SUCCESSFUL	Send	1,824	1,824	C:\Program Files\Afaria\Data\Ter
11/25/2008 5:04:38 PM	WM_Administrat8	SUCCESSFUL	Send	0	0	@C:\Program Files\Afaria\DATA\
11/25/2008 5:04:36 PM	WM_Administrat8	SUCCESSFUL	Send	2,932	2,932	C:\Program Files\Afaria\Data\Cha
11/25/2008 5:04:35 PM	WM_Administrat8	SUCCESSFUL	Send	0	0	C:\Program Files\Afaria\Data\Cha

Current view: File transfers for Client: WM_Administrat8 (9 Row(s)) Selected row: 6 More data

Right-clicking a row displays a shortcut menu from which you can view detailed history of the channel/channel set, as well as properties.

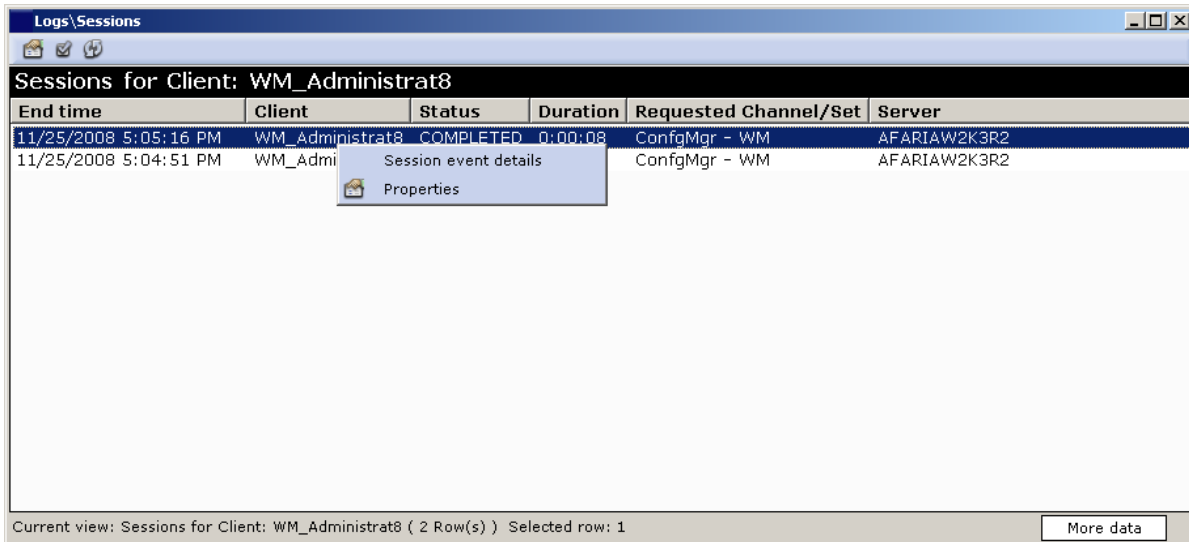


For information on event details, see [“Event Details for Logs Views”](#) on page 407.

To view properties for a selected row, see [“View Row Properties”](#) on page 408.

Sessions

Information that displays in this view includes the session end time; name of the client requesting the channel/channel set; status of the session; length of the session; channel/channel set requested by the client; and the name of the server sending the channel/channel set.



End time	Client	Status	Duration	Requested Channel/Set	Server
11/25/2008 5:05:16 PM	WM_Administrat8	COMPLETED	0:00:08	ConfigMgr - WM	AFARIAW2K3R2
11/25/2008 5:04:51 PM	WM_Admi			ConfigMgr - WM	AFARIAW2K3R2

Current view: Sessions for Client: WM_Administrat8 (2 Row(s)) Selected row: 1

More data

Right-clicking a row displays a shortcut menu from which you can view detailed history of the channel/channel set, as well as properties.



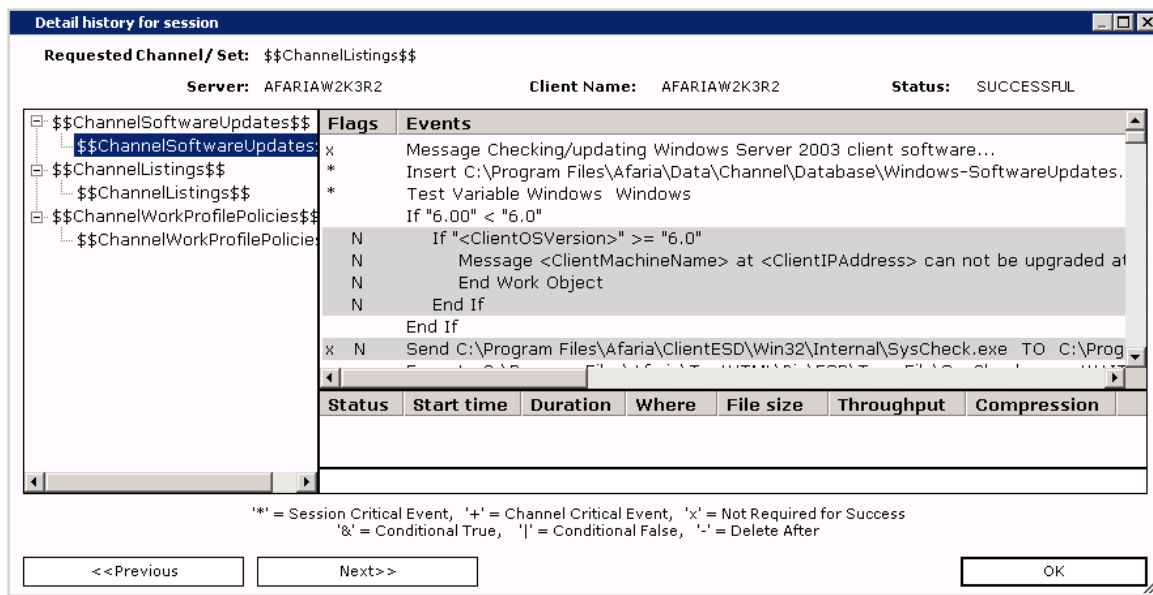
For information on event details, see [“Event Details for Logs Views” on page 407](#).

To view properties for a selected row, see [“View Row Properties” on page 408](#).

Event Details for Logs Views

When you view client data in the File transfers and Sessions mini-views, you have access to detailed session history. Right-click a row and then choose **Session event details** on the shortcut menu.

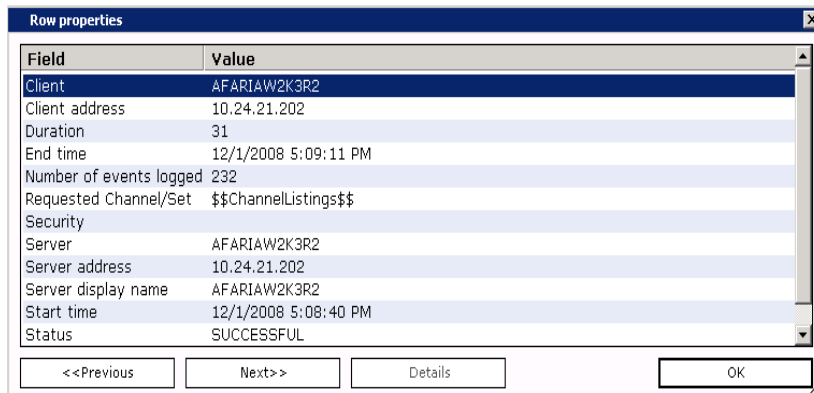
The fields at the top of the Detail history for session window present general information about the session including the name of the channel, the server that executed the session, the client that ran the channel, and the completion message for the entire channel. When the channel/channel set name is selected, the list displays the number of channel events and the overall completion status. When the channel/channel set name is expanded and a channel is selected, the list displays information at the event detail level.




Click **Close** to exit the window.

View Row Properties

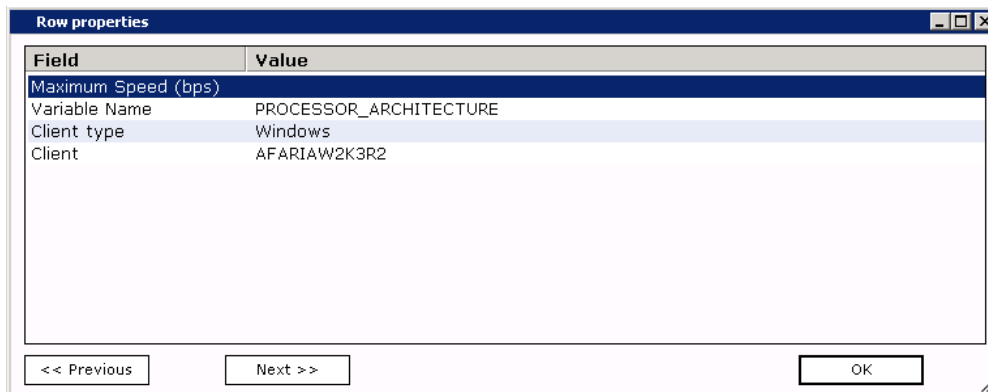
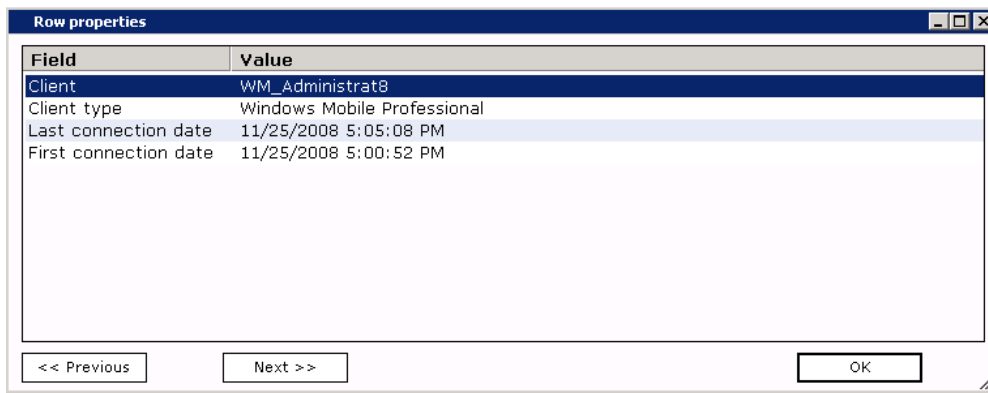
You can also view properties of any selected row in the File transfers and Sessions mini-views. Right-click the row and choose **Properties** on the shortcut menu. The Row properties window lists the fields in the row, as well as the value associated with each field. Click **Close** to exit the window.



Viewing Client Properties

To view the properties of any client in the right pane of Clients view, select the client to view and click  **Properties** on the button bar. You can also right-click the client and choose **Properties** on the shortcut menu.

The Row properties dialog box displays information specific to the selected row of the view. For instance, the dialog box immediately below presents row data from the predefined Windows view while the second dialog box presents row data from a custom view. The **Field** column represents the columns defined in the view, while **Value** represents the data returned by the column. The **Previous** and **Next** buttons in the lower part of the dialog box let you examine other rows in the view. Click **OK** to close the dialog box.



Changing a Client's Tenant Association

Change a client's tenant association to associate all of the client's future sessions with a different tenant. A client's associated data is also moved to the newly assigned tenant.

Change a client's tenant association only after defining the new tenant's client groups and operational assets, such as its profiles, policies, and channels. When the client connects to a new tenant, it is updated with the new tenant's profiles and no longer receives the prior tenant's profiles.

- 1 On a Data Views Clients page, right-click on a client in the right pane and select **Edit > Move to Tenant**.
- 2 Select a target tenant from the list.
- 3 Choose **OK**.

See also ["Using Multitenancy Features"](#) on page 25.

Changing a Device ID

Change a client's device ID (Afaria Device ID) as required for your needs. The Afaria Device ID displays in the Data Views Clients view and is an available column when you create custom views. Changing the value to something meaningful to your organization can help facilitate effective searching or help you build custom views.

1 Right-click a client in any Data Views view and choose **Modify > Change Device ID**.

2 Define the device ID naming convention:

- (Optional) Naming option – Select the field type to use to populate the device ID field. Clients must have selected inventory data in the database to use the inventory-based naming options. IMEI and IMSI data elements may not populate due to carrier- or power-state-dependencies that prevent the data from getting captured.
- (Optional) Prefix – Type a value to use as a prefix in the device ID field.
- Database value – This field is required when using the database naming option. Syntax is *TableName.ColumnName*.

The table must be defined in the Afaria database.

3 (Optional) Click **Preview** to view the result of your naming convention.

4 Click OK to commit the current naming convention change.

The resulting ID assignment is a static value; it does not automatically change if the value from the naming option changes.

Database specified value

The field requires syntax: *tableName.columnName*

Using the database specified value lets you add one custom value to the client's table. Use it to add a value that differentiates like-named clients but originates from data not represented by other naming options. Consider these items:

- It is your responsibility to ensure that the table, column, and row exist in the Afaria database.
- It is your responsibility to populate the table.
- The value is retrieved when you issue the command. The command always returns the first row of the table.

Deleting Client Data

Clients view allows you to remove specific data from a client, as well as a specific client from clients view. Data that you remove affects all of the views in Data views. Right-click the client and select **Delete**.

Remove all Client data deletes all information about the selected client. Selecting this option causes a full inventory scan the next time the channel connects to the server.

Remove backup data deletes data about this client from Data views, Backup.

Remove from all Client groups deletes the client from existing Static groups. Dynamic groups re-display a deleted client once the view is refreshed.



For information on creating client groups, see [“Client Groups” on page 284](#).

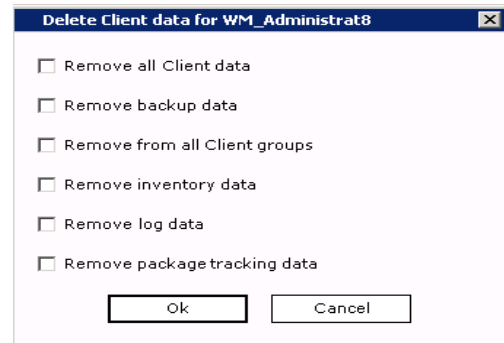
Remove inventory data deletes data about this client from Data views, Inventory. Selecting this option causes a new full inventory scan when the channel is run.

Remove log data deletes data about this client from Data views, Logs.

Remove package tracking data deletes data about this client from Data views, Package tracking.

Click **OK** to remove the data. You’re prompted to confirm the removal.

Click **Cancel** to close the dialog box without removing client data.



Combining a Client's Afaria Client ID



Use this feature with caution. This feature includes processes that permanently remove a client's record from the database in order to consolidate it with another client's record. It is possible to lose a client record that you intend to keep, without recourse.

The combine feature allows you to combine a current handheld client's data with a previous client of a like client type. The feature's intent is to allow you to recover from a circumstance in which reinstalling the Afaria software creates a new client identifier and therefore, a current client record that is without its former data. This condition occurs only when the Afaria Client device is un-serialized.



See ["About the Afaria client identifier" on page 48](#) to learn more about Afaria's unique client identifier, when and how it is created, and about its relationship to serialized and un-serialized devices.

Supported Client Types

The combine feature supports the following Afaria Client types:

- Palm
- Windows Mobile Professional (including Windows CE)
- Windows Mobile Standard

A Combined Client, Defined

A combined client is defined as the following combination of two, like-type clients records, subject to your installation's licensing and implementation:

- Previous client unique identifier
- Current client name
- Current client GUID
- Merged logs from previous and current client
- Previous client group assignments
- Previous client inventory data
- Previous client package tracking data
- Previous client license compliance data
- Previous client backup data
- Previous client user-defined data

This client definition simplifies the task of restoring a client after a reinstall and has the benefit of preserving its original history. Some data may be obsolete, depending on the state

of the current client. For example, if the client underwent a hard reset, then it may have lost some of its software inventory.

Combining Clients

Complete the following steps to combine clients.

- 1 Open a view on Data Views, Clients that contains the two, like-type clients of interest. It is recommended that you create a custom view to isolate the clients for easy viewing and to avoid an unintended reassignment.
- 2 Select the two clients and right click.
- 3 Select **Edit > Modify > Combine Clients**. The dialog provides a summary of the planned assignment for you to review. Afaria identifies the client with the most recent connection as the current client.

Warning: The two clients below will be combined into a new client.

Current Client	Previous Client
Name: WM_Administrat2	Name: Touch_Pro
Unique ID: 12	Unique ID: 11
GUID: {3FBF5000-7351-0801-3557-570150924440}	GUID: {3FBF5000-7351-0801-3583-530100935660}
Last Connection: 12/11/2008 12:20:05 PM	Last Connection: 12/10/2008 11:49:20 PM

New Client
Name: WM_Administrat2
Unique ID: 11
GUID: {3FBF5000-7351-0801-3557-570150924440}
Last Connection: 12/11/2008 12:20:05 PM

- 4 Choose Yes to accept the change. Afaria combines the clients to create a new, unified client and deletes the obsolete client data. Afaria logs successful reassignments in the Messages log.

About Outbound Notifications

Supported Client types – BlackBerry, Java, Symbian, Windows Mobile Professional (excluding Windows CE), Windows Mobile Standard, Windows

An outbound notification is a set of instructions that is sent from an Afaria server to a client. The instructions tell the client to initiate a connection back to its server to run a session. To send the notification, the server must use a client's IP or SMS address.

The outbound notification feature for Afaria clients requires that a "listener" is present at the client. The server delivers the listener to the client during the client's first connection. Therefore, a client must have had at least one successful Afaria connection before the client can receive an outbound notification.

Afaria includes a public Web service for the outbound notification feature so that you can offer the service without requiring access to your Afaria Administrator server. Contact your Afaria account representative for more information.

Managing Client Outbound Notification Addresses

Manage outbound notification address prior to sending outbound notifications. You can supply a specific IP or SMS address for a client. By default, the Afaria Server uses a client's last-known address.

See also ["About Outbound Notifications" on page 415](#).

- 1 Choose a view that displays a client list. Select one or more clients.
- 2 Choose **Client connection information**.
- 3 Update the **User IP address** or **SMS address** for the client if the **Last known IP** value is not current or is unknown. The dialog box displays the following information:

- Client name – The assigned name of the client device.
- Last known IP – The client IP address the server recorded during the last client connection.

Afaria uses this value for sending outbound notification if the user IP and SMS values are left blank. The value "Unknown" is appropriate for clients that support SMS notifications but not IP notifications.

- User IP address – An IP address to use to connect to the client. If defined, this value overrides the **Last known IP** value for making an outbound notification.
- SMS address – An SMS address to contact clients that support SMS. If defined, this value overrides the IP values for making an outbound notification.

The server sends future notifications using any overrides you defined and using last-known addresses for clients without overrides.

Client name	Last known IP	User IP address	SMS address
ENGWIN2K3VM	10.24.21.58		
XP-BLDG-1245-1	10.24.23.171		

Sending an Outbound Notification to Run a Channel

Send an outbound notification to run a channel to a client when you want the client to connect to an Afaria Server right away to request a specific channel. To run, the channel must be included in one of the client's group profile allowed channels list.

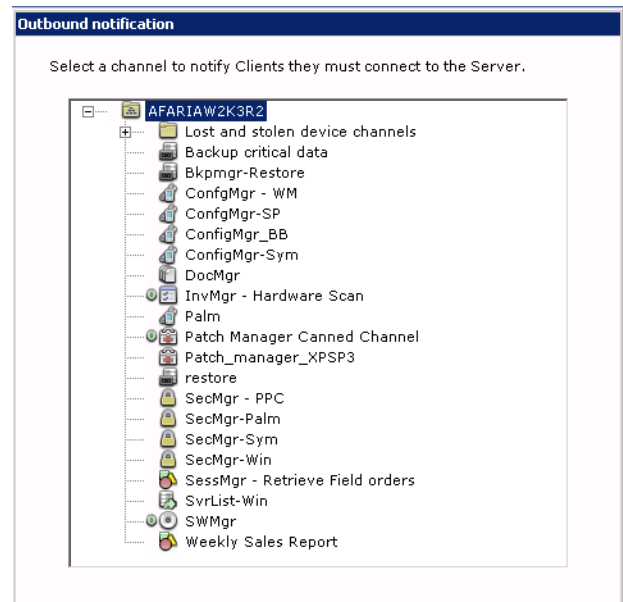
See also:

- [“About Outbound Notifications” on page 415](#)
- [“Managing Client Outbound Notification Addresses” on page 416](#)
- [“Profile – Allowed Channels” on page 240](#)

Data views > Clients > Outbound notification

- 1 Choose a view that displays a client list.
- 2 Select one or more Clients from the list.
- 3 Right-click and select **Outbound notification > Run Channel**.
- 4 Select a published channel that supports the client type for your selectionf.
- 5 Choose **OK** to send the notification.

If notification was successful, the client attempts to connect to the server and request the selected channel. The Messages log captures the success or failure of sending the outbound notification.



Sending an Outbound Notification to Apply Policies

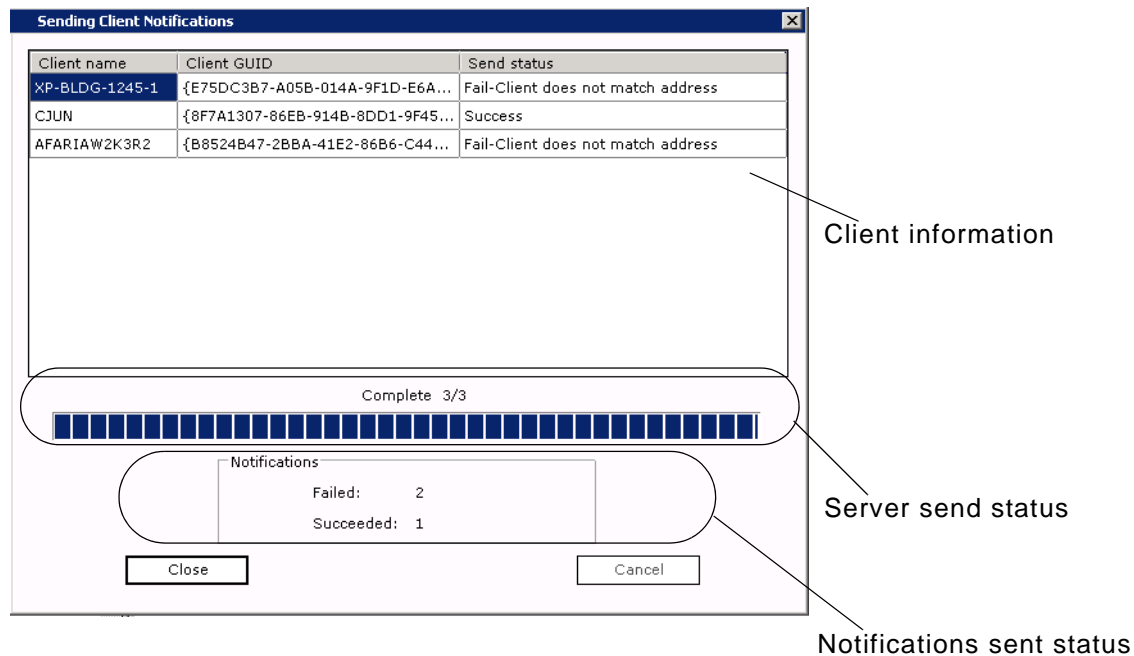
Send an outbound notification to apply a policy to a client when you want the client to connect to its server right away to receive its group profile and associated policies.

- 1 Choose a view that displays a client list.
- 2 Select one or more Clients from the list.
- 3 Right-click and select **Outbound notification > Apply Policies**.
- 4 Choose **OK** to send the notification.

If notification was successful, the client attempts to connect to the server. The Messages log captures the success or failure of sending the outbound notification.

Client Notifications Status

The Sending Client Notifications dialog opens after you send an outbound notification or remote wipe command to display the send status.



The status dialog reports the following status information:

Client information – Client information is a list of target clients. The Exchange column is included only for remote wipe command notifications that include the optional “Always block” setting.

Server send status – This status indicates progress and results for sending all the notifications or commands you initiated. The progress bar reflects the progress of the complete group of notifications, while the status text continually updates to indicate the progress and state of each client notification in the group of notifications. It is possible, for example, for connectivity issues to cause the server to fail sending individual notifications while completing processing on an entire group.

Notifications sent status – This status indicates the results of all the notifications that the Afaria Server was able to send out. It is possible, for example, for an Afaria Server to have the connectivity to successfully send an IP-based notification but report a failure status because the client was not logged on to the network to receive the notification.

Afaria Server captures the notification’s send success or failure in the Messages log.

If notification was successful, the client attempts to connect to the server and request the selected channel. The Messages log captures the success or failure of the outbound notification. The Sessions log captures the success or failure of the requested channel.

See also:

- [“Outbound notification” on page 161](#), to manage flood control and notification retries.
- [“Wiping a Remote Device” on page 422](#), for remote wipe feature and command.
- [“Exchange ActiveSync policy” on page 172](#), for Afaria Access Control for Exchange ActiveSync feature and configuration.

Sending BlackBerry Security Commands

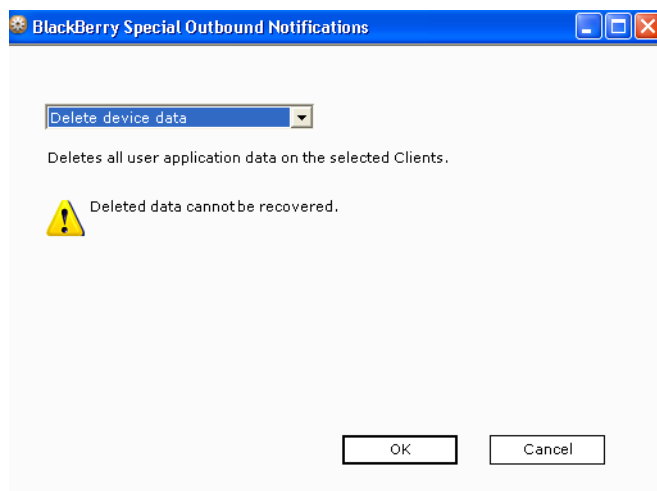
BlackBerry device control options are specialized outbound notifications. Using the options sends a set of instructions from an Afaria Server to an Afaria BlackBerry client. The instructions tell the client to execute some set of commands, as defined by the option you choose. Use the BlackBerry device control options to exercise specific security controls: delete device data, lock device, or unlock device.



Data loss – The delete device data option deletes application data, including Afaria's application and configuration data. It is comparable to using a BlackBerry device's Security > Wipe Handheld option. You must back up your device prior to executing the option in order to be able to recover the data. Use the BlackBerry Desktop Manager's Backup and Restore feature to facilitate backup and restore activity.

- 1 Choose a view that displays a client list. Select one or more clients from the list.
- 2 Open the context menu and choose **BlackBerry options**.
- 3 Select a control option and choose **OK**. Afaria supports the following controls:

- Delete device data – Also known as “Device wipe”. Delete all application data, including the Afaria Client application data.
- Lock device – Display a user message, disable all device I/O, and disable trackwheel. Device keys are disabled unless the user dials an emergency call. Afaria preserves the locked state through device resets and battery replacements.
- Unlock device – Remove user message, restore all locked features to an unlocked state.



Wiping a Remote Device

Client types supported are:

- Windows Mobile Professional 5 or later
- Windows Mobile Standard 5 or later
- Symbian

About the Remote Wipe Feature

The remote wipe feature is part of Afaria's core license that allows an Afaria administrator to send a device wipe command to an Afaria Client. The command is delivered in an SMS message. The command does not require user interaction to execute.

The remote wipe command always includes a hard reset action. The device's main memory is wiped of all data and applications that have been introduced since the device's last hard reset. The remote wipe command may include the following optional actions:



Windows Mobile advisory

- Windows Mobile – If you have disabled the device's external card through a Configuration Manager channel's Port Control feature, a remote wipe command that includes wiping the external data card will leave the card intact because the device cannot mount the card.
- Windows Mobile Professional 6.1 and later, Windows Mobile Standard 6.1 and later – If you have disabled SMS messaging through a Configuration Manager channel's Port Control feature, Microsoft messaging applications on the device will not receive the remote wipe command.

See *Afaria Reference Manual | Components*, Configuration Manager to learn more about disabling SMS messages and external data cards.

Symbian advisory

- Symbian clients – Some device types do not support hard reset with external card wipe. Therefore, the data on the external card may not be deleted before a hard reset. Test your device to be certain of hard reset behavior combined with the presence of an external card.
- External data card delete – Wipes the device's external data card of all data. The action executes only on a single, primary data card.
- Access control synchronization block – Windows Mobile only. Uses the Afaria Access Control for Microsoft Exchange feature to block the client device from synchronizing with the Exchange Server via Exchange ActiveSync synchronization requests. Synchronization requests can be sent from the client device but are denied before reaching the Exchange Server. See [“Exchange](#)

[ActiveSync policy](#)” on page 172 for more information about the Afaria Access Control for Microsoft Exchange feature.



- Remote wipe performs a hard reset on the device. In the unlikely event the remote wipe action cannot perform a successful hard reset due to operating system restrictions, the command executes an action to soft reset the device and display a user interface that the user cannot bypass. The device will require a hard reset to restore normal operations.
- Symbian – Some device types may briefly open a user-facing message before hard resetting. The hard reset occurs without requiring interaction from the user.
- It is recommended that you run a test on your device types to make a first-hand observation of the remote wipe command execution.
- Access policies – An administrator must have “create” rights for Data views > Clients in order to be able to execute a remote wipe command.

All instances of sending the remote wipe action to a client create a log message in the Messages log. Each log message identifies the action and the client.



Afaria includes a public Web service for the remote wipe feature so that you can offer the service without requiring access to your Afaria Administrator server. Contact your Afaria account representative for more information.

Overview of Remote Wipe Work Flow

The following steps are an overview of the remote wipe work flow.

- 1 An Afaria administrator uses the Afaria Administrator application (**Data views > Clients**) to select one or more clients for the remote wipe command. The administrator may choose to include the erase external data card and synchronization block actions.
- 2 The remote wipe command is sent to the client device by SMS address.
- 3 The client device receives the SMS message without any user interaction.
- 4 The remote wipe command, and any of its associated optional actions, executes without any user interaction.

Sending the Remote Wipe Command

- 1 Select one or more client rows in the data views results pane and open the shortcut menu.
- 2 Select **Remote wipe** to open the Remote wipe dialog box. The remote wipe command always includes a hard reset action. The device’s main memory is wiped of all data and applications that have been introduced since the device’s last hard reset. The remote wipe command may include the following optional actions:
 - External data card delete – Wipes the device’s external data card of all data. The action executes only on a single, primary data card.
 - Access control synchronization block – Windows Mobile only. Uses the Afaria Access Control for Exchange ActiveSync feature to block the client device from synchronizing with the Exchange

Server via Exchange ActiveSync synchronization requests. Synchronization requests can be sent from the client device but are denied before reaching the Exchange Server.

3 Choose **OK**.

See also:

- [“Client Notifications Status” on page 419](#), for information about the Sending Client Notifications dialog that follows issuing a remote wipe command.
- [“Outbound notification” on page 161](#), to manage flood control and notification retries.
- [“Exchange ActiveSync policy” on page 172](#), for Afaria Access Control for Microsoft Exchange feature and configuration.

Recovering a Data Security Manager Client Password

Recover password allows you to provide recovery support to Afaria Data Security Manager for handheld client users.

Use the recover password feature for issuing a temporary recovery password to a client user that has a device but has forgotten the password. The new, temporary password is valid for a single log on. Afaria directs the user to create a new password as soon as they use the temporary password to gain entry to the Data Security Manager client.



Afaria includes a public Web service for the password recovery feature so that you can offer the service without requiring access to your Afaria Administrator server. See *Afaria Reference Manual | APIs*.

The recovery feature is enabled only for Afaria Data Security Manager clients, both handheld and Windows Data Security Manager clients. Afaria uses the password recovery dialog box in a default state to start the process, and then in the password state after generating the password. The Windows client recovery process differs from the handheld client recovery process.

Password recovery for handheld clients

Temporary password recovery

Enter the Client recovery key and click "Generate" to recover the temporary password.

Client Powen

Client recovery key

Temporary password

Generate Cancel

Recovery dialog - default state

Temporary password recovery

Enter the Client recovery key and click "Generate" to recover the temporary password.

Client Powen

Client recovery key

Temporary password

Generate Cancel

Recovery dialog - password state

Password recovery for Windows clients

Temporary password recovery

Enter the last 3 pairs of digits of the challenge code for the client below. Click "Generate" to generate the Response code.

Client CJXP

Challenge code digits

Response code

Generate Cancel

Recovery dialog - default state

Temporary password recovery

Enter the last 3 pairs of digits of the challenge code for the client below. Click "Generate" to generate the Response code.

Client CJXP

Challenge code digits

Response code

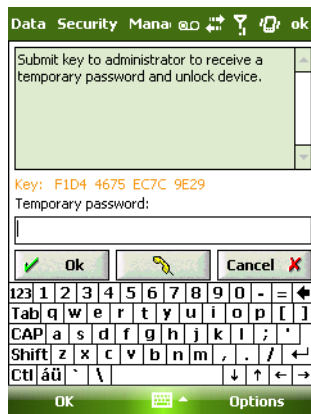
Generate Cancel

Recovery dialog - password state

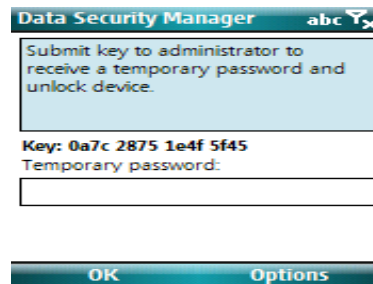
Recovering a Password for Handheld Clients

Afaria Data Security Manager for handheld clients lets you issue a temporary password for a user to enter on the Data Security Manager client's temporary password screen. Users can make phone calls during the password recovery process.

Sample temporary password screens



Windows Mobile Professional



Windows Mobile Standard



Symbian



Palm

Data Security Manager for handhelds - Password Recovery Process

This process describes the order of events for issuing a temporary password for users that have forgotten their passwords, but still have ownership of their clients.

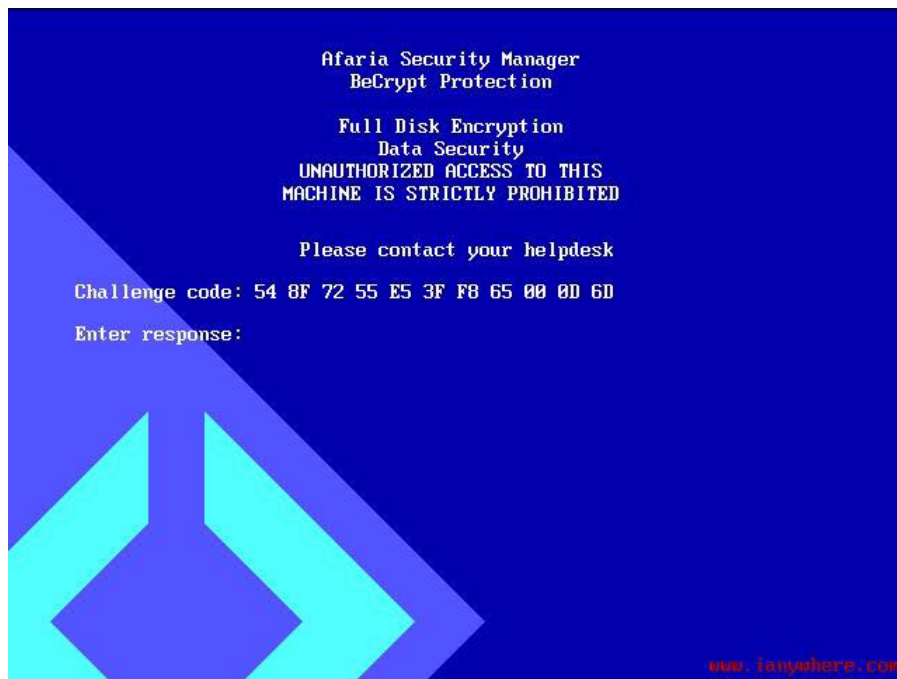
Step	Administrator	Client user
1		<p>Open the temporary password screen. This screen includes a broadcast message to advise a user to contact an administrator for password recovery support. You can use the Data Security Manager Channel Editor to customize this message for some clients. The screen also provides a key value to use for generating the temporary password.</p> <p>Opening this screen starts a 10-minute timer on the client, after which the key value and the resulting temporary password are invalid. The client notifies the user if the timer expires. The notification allows the user to restart the timer and receive a new key value.</p>
2		<p>Follow instructions for contacting support. Provide device key from the Forgot Password screen.</p>
3	<p>Open the Afaria Administrator console and select Data View > Clients > All Clients. Select the client, open the shortcut menu and choose Recover password... to open the recovery dialog box.</p>	
4	<p>Type the key in the client recovery key field and choose Generate. The Temporary password field populates with a new, temporary password.</p> <p>The client's recovery password key and the Afaria Administrator's generated temporary password are in hexadecimal format (0-9, A-F).</p>	
5	<p>Communicate temporary password to user. Ensure that they make proper hexadecimal data entry.</p>	
6		<p>Use the new password as the Temporary Password. If the password fails, verify accurate hexadecimal data entry or restart the process with a new key value and new temporary password.</p>
7		<p>Follow prompts to create a new password.</p>

Recovering a Password for Windows Clients

The password recovery process for Data Security Manager Windows clients allows you to issue a response code for a user to type as their response to the Security Manager client's challenge code. The client exposes the challenge code when the client is in a state of denied access.




With the release of Afaria 6.0, Security Manager has been renamed to Data Security Manager to more closely reflect its role in the Afaria product suite. Due to integration with third-party components, all user-facing references in Windows client components remain "Security Manager" for the current release.



State of denied access - Client screen sample

Data Security Manager for Windows - Password Recovery Process

This process describes the order of events for issuing a response code for a user whose Security Manager client is in a state of denied access with a challenge code exposed.

<i>Step</i>	<i>Administrator</i>	<i>Client user</i>
1		The client enters a state of denied access when a user fails the Security Manager authentication process too many times. The threshold for authentication failures is defined by the security policy. The state of denied access presents the user with a challenge code to which they must reply with a valid response code in order to regain access to the Security Manager client.
2		Contact support administrator. Provide the administrator with the first eight pairs of characters from the challenge code from the client screen and the client's computer name to help them retrieve your client information.
		
3	Use the Afaria Administrator application to locate the client in a data view by choosing Data View > Clients > Windows Clients and searching for the client row with a client name and challenge/response code value that matches the client of interest.	
4		Provide the administrator with the last three pairs of characters from the challenge code from the client screen.
		

Data Security Manager for Windows - Password Recovery Process (Continued)

This process describes the order of events for issuing a response code for a user whose Security Manager client is in a state of denied access with a challenge code exposed.

<i>Step</i>	<i>Administrator</i>	<i>Client user</i>
5	<p>Open the client's context menu and choose Recover Password to open the Temporary password recovery dialog.</p> <p>Type the last three pairs of digits from the challenge code on the client screen in the Challenge code digits data boxes and choose Generate. The dialog's Response code data box populates with a response code.</p> <p>The client's challenge code and the Afaria Administrator's generated response code are in hexadecimal format (0-9, A-F).</p>	
6	<p>Communicate response code to user. Ensure that they make proper hexadecimal data entry.</p>	
7		<p>Use the response code to reply to the challenge code.</p>
8		<p>Follow prompts to change password after the computer boots and you log on to Windows.</p>

Managing Data Security Manager Administrator Accounts

The Data Security Manager for Windows (Data Security Manager) administrator account is an account on the client computer that has Data Security Manager administrative rights if the account also has Windows administrative rights. The account is created during the Data Security Manager account installation. The account information is sent to the Afaria Server after it is created. However, no further account tracking occurs after the installation is complete.



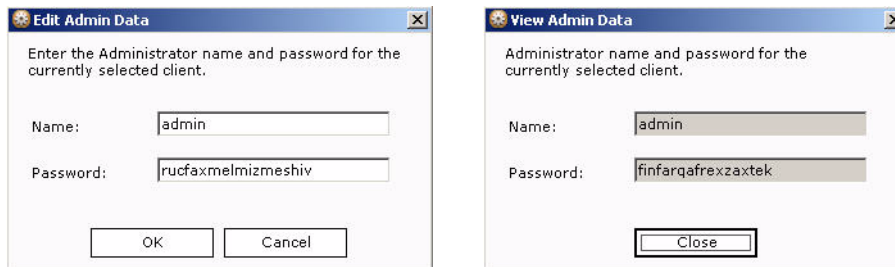
Tracking the Data Security Manager client's administrator account name and password, after the initial value is populated, is a manual process. Therefore, there is the potential to create a mismatch between the administrator data at the Afaria Server (Data Views) and the administrator data at the client. You must manage Data Security Manager administrator account information at the Afaria Server any time you update the account at the client.

Modify Data Security Manager administrator accounts information in either of the following cases:

- The account password has changed. In this case, change only the password value.
- You want to change the Data Security Manager administrator account that you want to track. In this case, change the account name and password values.

To modify and view account information:


- 1 Choose a view that displays the Data Security Manager client of interest.
- 2 Select the client's row, open the context menu, and select **Edit Admin Data** or **View Admin Data** to open the data dialog.

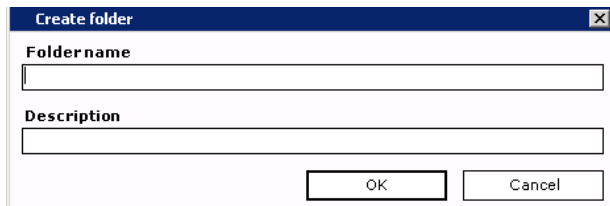


Sample dialogs

- 3 Change or view data according to your need. This data is not verified upon entry. Password values are stored in an encrypted state.

Creating a New Client Folder

Click  **New**, then select **Folder** to open the Create folder dialog box. Enter a **Name** and **Description**, then click **OK**.




The image shows a 'Create folder' dialog box with a title bar containing a close button. It has two text input fields: 'Folder name' and 'Description'. At the bottom, there are two buttons: 'OK' and 'Cancel'.

The folder displays in the left pane of Clients view.

Creating a Custom Client View

Supported client types – Afaria Clients

Create custom database views to return data from the database that is not already represented in a predefined view. To create a new client view, select the top node in the clients tree and click  **New**, then select **View**. The View editor dialog box appears. Use it to label and create/manage columns in the view.

See also [“Creating Custom Database Views” on page 389](#) and [“Viewing a Custom View’s SQL Statement” on page 393](#).

Renaming a Folder or View




You cannot alter the name/description of predefined folders or views.

To edit the name or description of a folder or view, right-click the item and then choose **Rename** on the shortcut menu. The Rename dialog box displays the item’s original name and description.

Edit the **New name** or **Description** fields, then click **OK**.

Viewing Folder or View Properties

You can view the properties of a selected folder or view by clicking  **Properties** on the button bar or right-clicking the item and choosing **Properties** on the shortcut menu.



Creating a Group Within a View

To create a group, right-click any view and then choose **New, Group** on the shortcut menu.

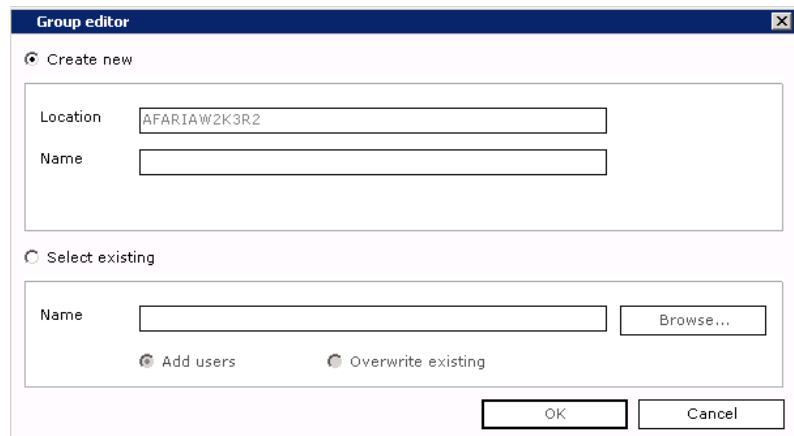
NT/LDAP groups

When you select **NT/LDAP** on the shortcut menu, the Group Editor dialog box for your server appears through which you can create new or select existing NT or LDAP groups. Once created, you can manage these groups through the operating system on which the server is installed.

NT

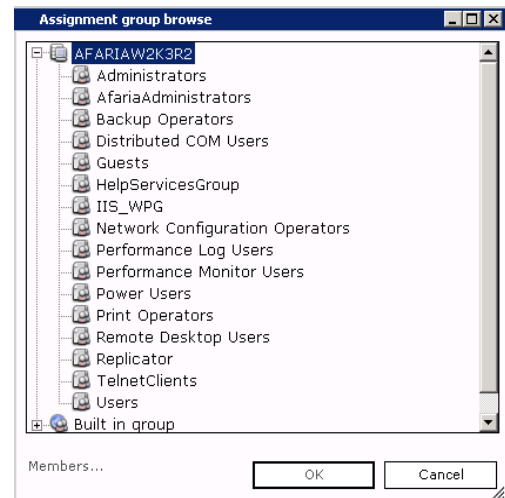
Creating a new group is the default. **Location** defaults to the installed server. Enter the **Name** of the group.

Local (default) allows you to create a group from specific NT user groups. **Global** allows you to create a group from the global NT domain.



To use an existing group, select the **Select Existing** radio button and then click **Browse**. The Assignment Group Browse dialog box appears. Expand the list to locate the group.

To view the members of a group, select it and then click **Members**.



Use the read-only Group members dialog box to view group information.

Name	Full name	Description
ASPNET	ASPNET	
Authenticated Users	Authenticated Users	
helpdesk	helpdesk	
INTERACTIVE	INTERACTIVE	

Name. Domain, or name of the group.

Description. Representation of the group, such as “Marketing.”

Members. The name, full name, and description of all group members.

Click **OK** to save the group name to the Name field in the Group Editor dialog box.

Create new

Location: AFARIAW2K3R2

Name:

Select existing

Name: Users [Browse...]

Add users Overwrite existing

[OK] [Cancel]

Click **OK** to close the Group Editor dialog box.

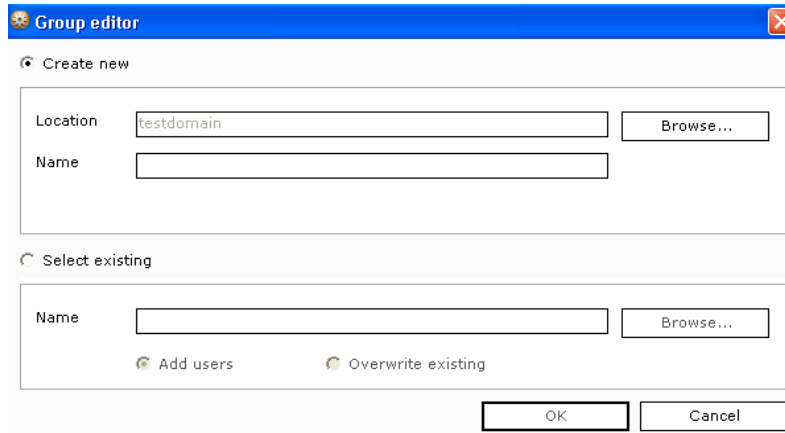


Afaria Server installed in a Domain Controller that contains the directory data store – Clicking **OK** saves the new group to the operating system on which the server is installed, therefore the new group isn't visible in Clients view. Manage the group using the Administrative Tools provided by the operating system.

Afaria Server installed as a domain member – Clicking **OK** saves the new group to a Domain Controller directory.

LDAP Groups

Creating a new group is the default.



Location defaults to an organizational unit in the LDAP directory, but you can click **Browse** to select another group in the Assignment Group Browse dialog box.

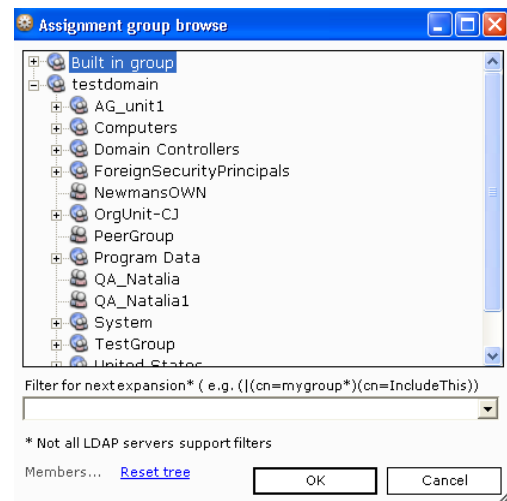
Select a group and then click **OK** to return to the Group Editor dialog box.

Enter a **Name** for the group.

To use an existing group, select the **Select Existing** radio button and then click **Browse**. The Assignment Group Browse dialog box appears. Expand the list to locate the group.

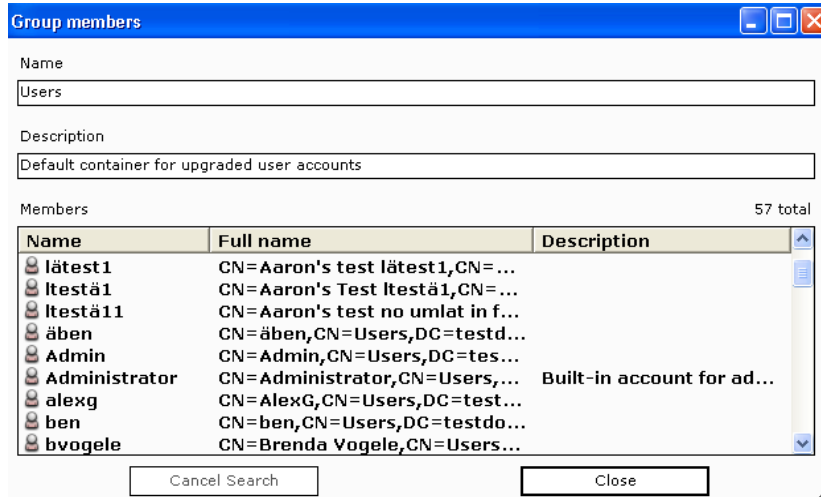
To use a defined LDAP filter, enter it in the LDAP filter field.

To view the members of a group, select it and then click **Members**.



Use the read-only Group members dialog box to view all the members of the organizational unit you selected from the directory tree in the Assignment Group Browse dialog box.

LDAP servers place limits on how many entries you can view at once. If a group contains a large number of users, the list may be truncated by the LDAP server.

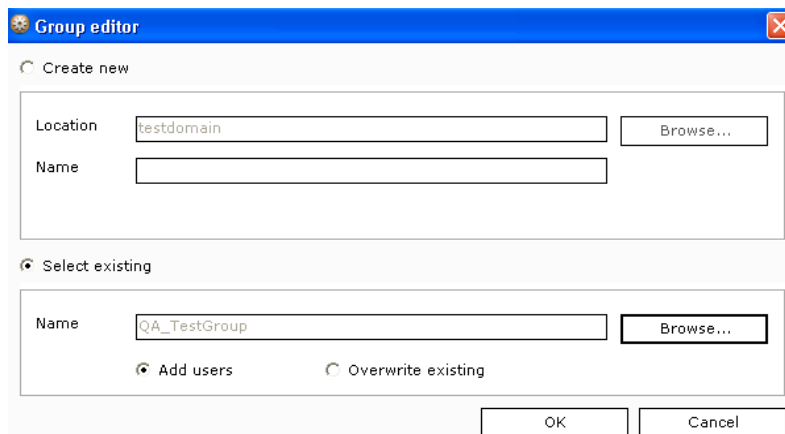


Name. Root to which the unit belongs, such as “mycompany.com.”

Description. Name of the organizational unit, such as “Human Resources.”

Members. The user’s name, full name, and description of all members of the selected group.

Click **OK** to save the group name to the **Name** field in the Group Editor dialog box.



Click **OK** to close the Group Editor dialog box.



Clicking **OK** saves the new group to the operating system on which the server is installed, therefore the new group isn’t visible in Clients view. Manage the group using the Administrative Tools provided by the operating system.

Dynamic Client Groups

When you select **Dynamic Client groups** on the shortcut menu, the Dynamic Client group dialog box appears through which you can create new client groups.

Enter the name and description of your group and then click **OK**.

See “Client Groups” on page 284.

Creating a New SQL View Within a View

Right-click any view and then choose **New, SQL View** on the shortcut menu. Use the New view dialog box to create a new SQL view in the database where your server is installed. Enter a valid SQL view **Name** and then click **OK**.



Clicking **OK** saves the new view to the database used by the server; therefore, the new view isn't visible in clients view. Manage the SQL view using the tools provided by the database.

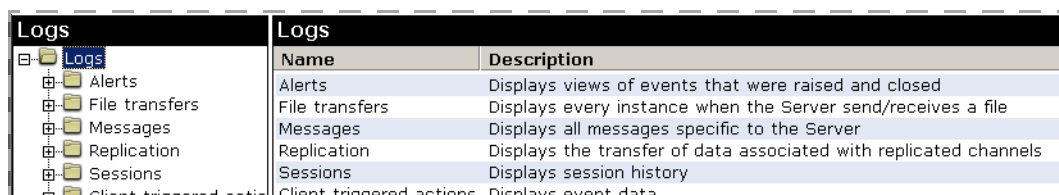


Working with Logged Actions

Logs view allows you to examine occurrences of any action that affected the server. Logs view contains two panes:

- The left pane displays predefined folders that contain a variety of views. You can use these or you can define your own folders and views within one of the predefined folders.
- The right pane displays data specific to the item selected in the left pane.

Data views > Logs



Logs	
Name	Description
Alerts	Displays views of events that were raised and closed
File transfers	Displays every instance when the Server send/receives a file
Messages	Displays all messages specific to the Server
Replication	Displays the transfer of data associated with replicated channels
Sessions	Displays session history
Client triggered actions	Displays event data

Information Collected by Predefined Views

Logs view contains predefined folders. Each folder includes a variety of views that collect specific information about server, client, or partner servers.



The type of data that displays in the Messages, Replication, Sessions, Client triggered actions, and Client deployment folders depends upon the logging policies you set on the Server configuration, Properties, Logging policy page. For information on setting logging policies, see [“Logging policy” on page 135](#).

Data that displays is removed after the number of days defined on the Server configuration, Properties, Log cleanup page. For information on setting log cleanup options, see [“Log cleanup” on page 138](#).

Alerts

The Alerts log includes events that were raised, as well as a view of the alerts that were closed.

- Raised events – Includes the name of the event; computer on which the event occurred; time the event occurred; time the event was received at the server; any relevant details; component-specific error code associated with the event; and server that received the event.
- Closed alerts – Includes the name of the alert; name of the contact (if any) assigned to the alert; time the alert was raised, acknowledged, or closed; any closing remarks the contact had about the alert; identification number assigned to this alert; and server that received the alert.

File transfers

The File transfers log includes every instance of the server sending or receiving a file. The right pane displays the date and time this event stopped transferring the file; server that originated the transfer; completion status or error type: SUCCESSFUL or FAILED; path from which the server downloads information to the client; total number of kilobytes (handheld clients) or bytes (Windows clients) in the file being transferred; and number of kilobytes/bytes successfully transferred.

- All – Includes all file transfer information such as all attempts to upload or download files, or the status of past communications sessions.
- Failed – Includes all failed file transfers or sessions.
- Sorted by Channel – Includes all file transfers, sorted by channel.
- Sorted by Client – Includes all file transfers, sorted by client or client group.

Messages

The Messages log includes all of the server's User, Information, Fatal, Debug, and Error messages that are specific to the server. The right pane displays the date and time the message was logged at the server with the most recent message displayed at the top; type of message; administrator assigned to the server; server on which the message was recorded; and message received at the server. Message type includes, USER (messages generated by a Session Manager Message event); INFO (messages about the server); FATAL (messages indicating a critical error of an application); and ERROR (messages indicating usage or formatting errors).

- All – Includes all actions taken by the server such as features enabled, channels created, and channels edited.
- Errors – Includes all errors that occurred at the server.
- Errors in session – Includes all errors that occurred at the server, sorted by session.

OMA DM messages

Afaria captures OMA DM session return codes in the Messages log:

- 0 – No error.
- 1001 – The Afaria OMA DM server encountered a situation from which it cannot recover. This may be due to authentication problems or device return codes to one or more OMA DM commands, or something else. A more descriptive code is returned when possible.
- 1002 – The client requested to abort the session. It may occur due to multiple authentication failures, or possibly due to unsupported or unrecognized OMA DM commands.
- 1003 – Reserved for future use.
- 1004 – The client failed several authentication attempts.
- 1005 – The same as 1002.

- 1006 – The transmission of a large object to the client failed. Typically, this is an executable file that an SCM policy is installing.
- 1007 – The policy is unable to locate an OMA DM object that is required for success. For example, an access point object referenced from the SCCP policy is not found at the client.
- 1008 – Reserved for future use.
- 1009 – The policy is unable to locate an OMA DM object node that is required to provide information for another node's value. This is slightly different from 1007, and is rarely observed.
- 1010 – Internal error. An exception is caught by the main method in the session handler of the OMA DM server.
- 1011 – Internal error.
- 1012 – A variable used in a policy is resolved. Typically, this results from an error in the definition of a free-form policy.
- 1013 – An SCM install action failed.
- 1014 – The communication with the Afaria Session Manager failed. Typically this occurs when the Afaria Server becomes unavailable during an OMA DM session, or when the Afaria session times out.

Replication

The Replication log includes User, Information, Fatal, Debug, and Error messages that are specific to replication. The right pane displays the date and time when replication occurred with the most recent entry displayed at the top; type of message; server on which the message was recorded; name of the server partner to which or from which channels are replicated; and message received at the server. Message type includes, USER (messages generated by a Session Manager Message event); INFO (messages about the server); FATAL (messages indicating a critical error of an application); and ERROR (messages indicating usage or formatting errors).

- All – Includes all actions and components involved in replication.
- File transfers – Includes information about the transfer of data associated with replicated channels.
- Sessions – Includes information about each session.

Sessions

The Sessions log includes information about past sessions. The right pane displays the date and time when the session with the client ended; completion status or error type: SUCCESSFUL, COMPLETED, or FAILED; session duration in hours, minutes, and seconds; channel or channel set requested by the client; server to which the client connected; and client computer that connected to the server.



Information about OMA DM Clients are captured in a session's event details. See ["Viewing Session Event Details"](#) on page 449.

An entire channel set's sendlist processing is aggregated into a single unit and occurs with the first sendlist instance in the channel set. Therefore, all of the sendlist Sessions logging for a channel set occurs with the first channel in the set that contains a sendlist.

- All – Includes all session information such as all attempts to upload or download files, or the status of past communications sessions.
- Failed – Includes all failed sessions.
- Sorted by Channel – Includes all sessions, sorted by channel.
- Sorted by Client – Includes all sessions, sorted by client or client group.

Client triggered actions

The Client triggered actions log includes event monitors that record successes or failures for associated monitor-action pairs that occur on a client. The success or failure of a pair is defined as whether the specified action was initiated successfully, or that the action not only started, but completed and returned a success status.



Windows clients, initial connection not logged – The client does not log the connection action that was initiated by a new client package's "initial connection" setting.

- All – Includes all actions and data associated with a client action. Information includes:
 - Client name
 - Completion date and time stamp



Clients/Servers subject to Daylight Saving Time – When either the client or a server reside in a time zone that is subject to Daylight Saving Time, it is possible for the log to reflect a time stamp that is an hour ahead or behind the time the event actually occurred.

- Action type
- Status
- Associated data
- Monitor name
- Monitor type

- Monitor's variable data values
- Log only actions – Includes only logging actions and data associated with a client action. Information includes:
 - Client name
 - Event time
 - Monitor name
 - Monitor type
 - Monitor's variable data values
 - Associated data

See [“Profile – Client Actions” on page 233](#) for information on monitor-action pairs in group profiles. See [“Logging policy” on page 135](#) for information on client action logging services and [“Log cleanup” on page 138](#) for information on cleaning up Client actions logs.

Client deployment

The Client deployment log includes client deployment status tracking information from previous sessions. The right pane displays specific information fields as follows:

- All – Includes all client deployment status tracking events that occurred at the server including:

Date/Time	Notification ID	Message
Sent verification	Download verification	Connected verification
Error in sending	Error in download	Error in connection
Cancelled send	E-mail address	Package ID
File ID	First Name	Last Name
Error occurred		

- Errors – Includes client deployment status tracking events containing errors that occurred at the server including:

Date/Time	Notification ID	Error in sending
Error in download	Error in connection	Message

Handheld Security

The Handheld Security log includes security-related messages for handheld clients. The Afaria Client collects Bluetooth connection activity events as they occur on the client, and then delivers the collection to the Afaria Server during Afaria sessions. Use the Handheld Security log to learn:

- Date – The date and time of the logged event.

- Client – The name of the client on which the logged event occurred.
- Type – The kind of message logged, e.g., information, warning, or error.
- Message – A description of the logged event, which includes the Bluetooth device type and whether the Bluetooth connection succeeded or failed.

Windows Security


The Windows Security log includes security-related messages for Windows clients. The Afaria Client collects security events as they occur on the client, and then delivers the collection to the Afaria Server during Afaria sessions. Use the Windows Security log to learn:

- Date – The date and time of the logged event.
- Client – The name of the client on which the event occurred.
- Type – The kind of message logged, e.g., information, warning, or error.
- Message – A description of the logged event.

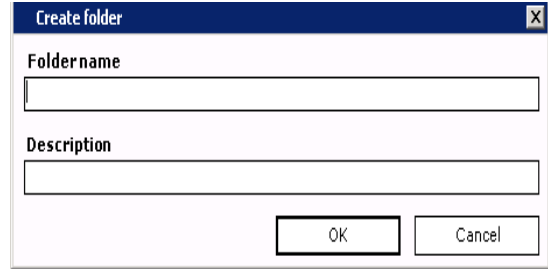
Policy Delivery

Displays views related to policy delivery and updates. Logs record the nature and status of a policy and whether updates succeeded, failed, or deleted the policy.

Creating a New Log Folder

You can “nest” new folders within a predefined folder to create a hierarchical structure. Select the parent folder, click  **New**, then select **Folder** to open the Create folder dialog box.

In the Create folder dialog box, the read-only Parent folder field displays the intended location for the new folder. Enter a **Folder name** and **Description** and then click **OK**. The folder is saved under the parent folder in Logs view.




If you want to change the location of the new folder, you must close the Create folder dialog box and select another parent folder.



For information on renaming a folder or view, [“Renaming a Folder or View” on page 446](#)

Creating a Custom Log View

Create custom database views to return data from the database that is not already represented in a predefined view. To create a view within a predefined/custom folder, select the parent folder, click  **New**, then select **View** on the button bar. You can also right-click the parent folder and choose **New, View** on the shortcut menu. The View editor dialog box appears in which you label and create/manage the columns in the view.

See also “Creating Custom Database Views” on page 389 and “Viewing a Custom View’s SQL Statement” on page 393.

Renaming a Folder or View




You cannot alter the name/description of predefined folders or views.

To alter the name and/or description of a folder or view, right-click the item and then choose **Rename** on the shortcut menu. The Rename dialog box displays the item’s original name.

The screenshot shows a dialog box titled "Rename" with a close button (X) in the top right corner. It contains three text input fields: "Original name" with the text "Custom", "New name" with the text "Custom", and "Description" with the text "Sessions". At the bottom of the dialog box, there are two buttons: "OK" and "Cancel".

Make alterations in the **New name** and/or **Description** fields, then click **OK**.

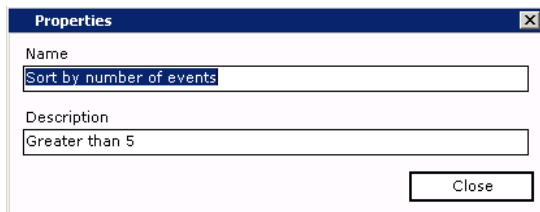
Viewing Folder or View Properties

You can view the properties of a selected folder or view by clicking  **Properties** on the button bar, or right-clicking the item and choosing **Properties** on the shortcut menu.

The dialog box below represents a folder’s properties.

The screenshot shows a dialog box titled "Properties" with a close button (X) in the top right corner. It contains two text input fields: "Name" with the text "Custom" and "Description" with the text "Sessions". At the bottom of the dialog box, there is a button labeled "Close".


The second dialog box represents a view’s properties.



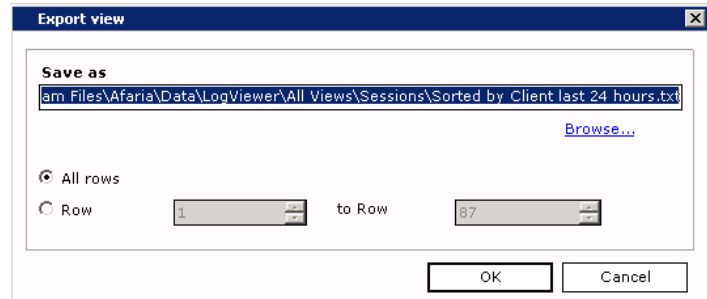
The image shows a 'Properties' dialog box with a dark blue title bar and a close button (X) in the top right corner. The dialog contains two text input fields. The first field is labeled 'Name' and contains the text 'Sort by number of events'. The second field is labeled 'Description' and contains the text 'Greater than 5'. A 'Close' button is located at the bottom right of the dialog.

Field	Value
Name	Sort by number of events
Description	Greater than 5

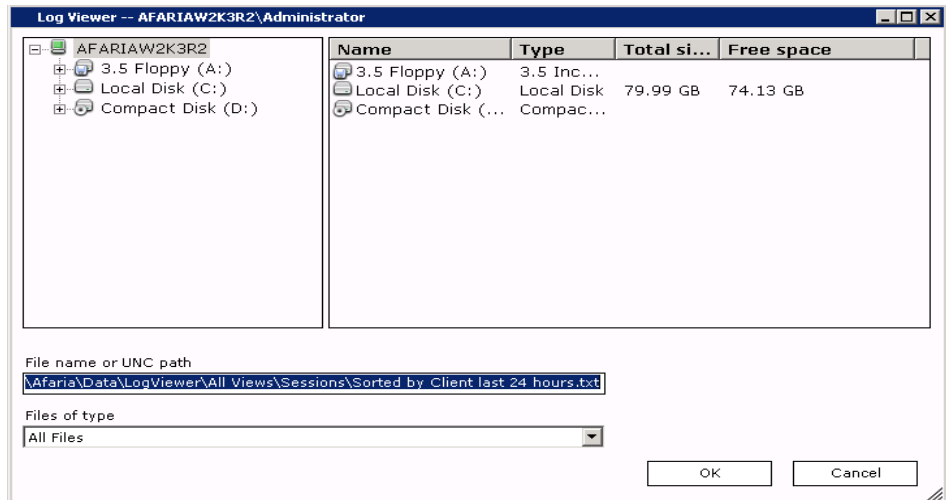
Exporting a Log View

To export log views and save them as text (*.txt) files in another location, right-click a view in the left pane, then choose **Export** on the shortcut menu. You can also select the view and click  **Export** on the button bar.

In the Export View dialog box, **Save as** field, enter the path where you want to save the export text file.



You can also click **Browse** to open the Log Viewer dialog box in which you can locate the folder in which to save the view.




In the Export View dialog box, determine whether to save all of the rows, or a specific number of rows.

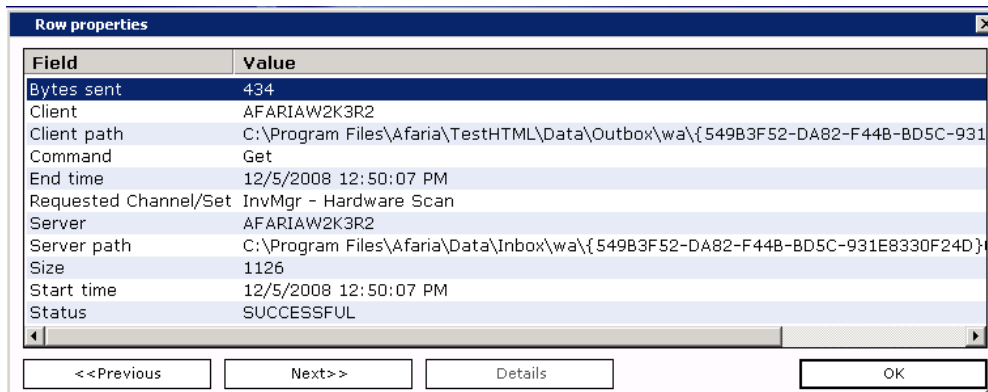
All rows saves all of the rows of the log view.

Row to Row allows you to save disk space by entering a range of rows to save.

Click **OK** to export the view and return to Data views, Logs.

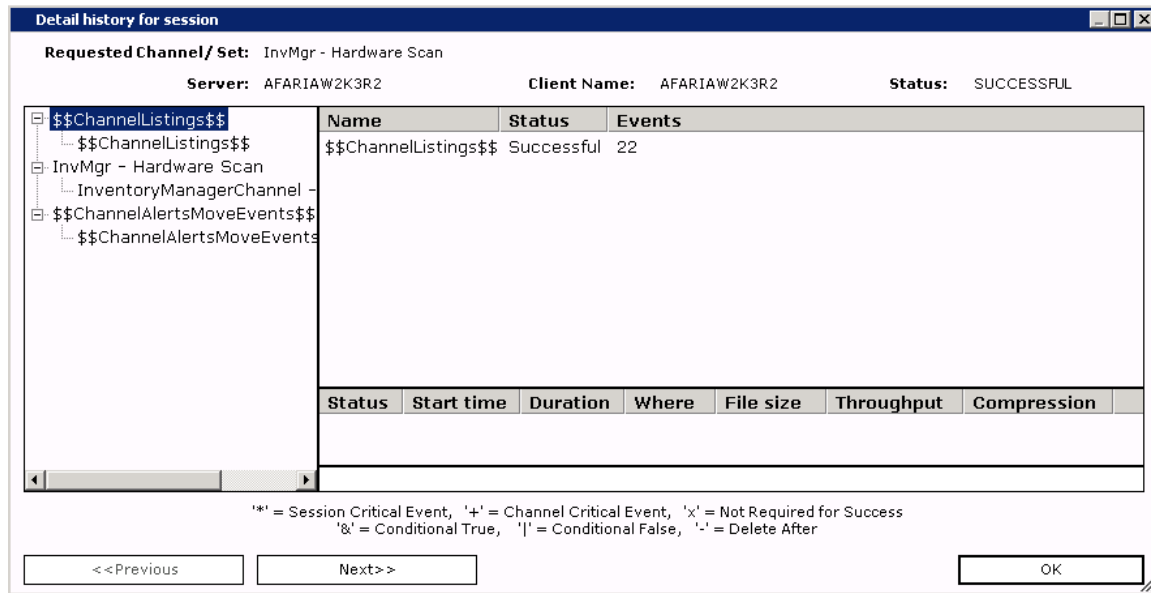
Viewing Row Properties

To view row properties of any Logs view, select a view (left pane), then select the row to view in the right pane. Click  **Properties** on the button bar, or right-click the row and choose **Properties** on the shortcut menu. The Row properties dialog box displays information specific to the selected row of the view. The **Field** column represents the columns defined in the view; **Value** represents the data returned by the column. The **Previous** and **Next** buttons allow you to examine other rows in the view. Click **OK** to close the dialog box.



Viewing Session Event Details

Views in the File Transfers and Sessions folders provide detailed log entries. To access this information, select a view (left pane). When results display in the right pane, right-click the row to examine and then choose **Session event detail** on the shortcut menu. The Detailed history for session dialog box appears.



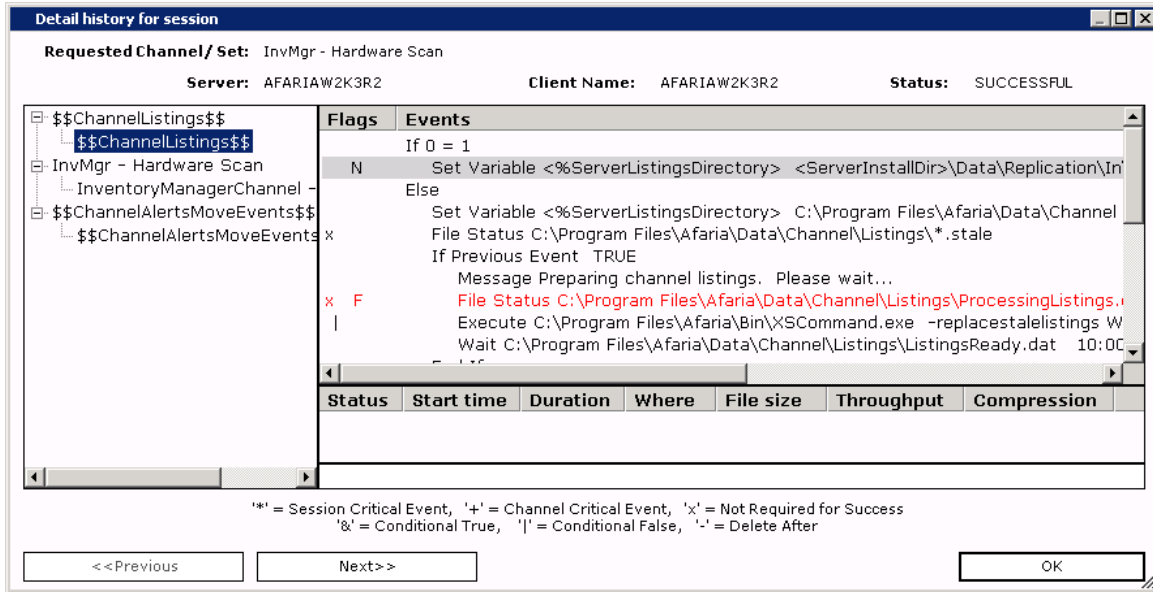
The fields at the top of the dialog box present general information about the session including the name of the channel, the server that executed the session, the client that ran the channel, and the completion message for the entire channel.

When the channel/channel set name is selected, the list displays the number of channel events and the overall completion status.

When the channel/channel set name is expanded and a channel is selected, the list displays information at the event detail level.

- The **Flags** column displays symbols that represent why an event failed. Event flags represent:
 - &** **Conditional True** indicates that the event will execute only if the previous event returned a true value or was successful.
 - |** **Conditional False** indicates that the event will execute only if the previous event returned a false value or failed.
 - *** **Critical Event** an “F” flag next to this event indicates the source of a critical failure.
 - **Delete After** indicates that the file in the event after this event has successfully executed.
 - F** indicates that the event failed.
 - N** indicates that this event never executed.

- The **Events** column displays the evaluated event. The server evaluates variables and conditional statements during start time and substitutes the values in the event history detail.



Working with Client Inventory Data

Inventory view is the central location to view retrieved client inventory data collected through Inventory Manager channels. Inventory view contains two panes:

- The left pane displays three predefined folders. Change detection views allows you to monitor specific inventory changes for clients. Custom Views allows you to create new folders and views within that parent folder. Once created, you can edit, rename, and delete these folders and views. Inventory Views displays detailed inventory data unique to each client type.



Right-clicking an item displays a shortcut menu. Option availability depends upon the selected item, for instance the only option available for a view in the Change Detection Views folder is Configure Change Detection.

- The right pane displays data, in column format, specific to the item selected in the left pane. Custom folders display name and description; custom views display client name and data specific to the parameters that you define.



Right-clicking a row displays a shortcut menu. Depending upon the row selected, you can acknowledge changes or view client hardware/software inventory data. For Windows clients you can also view directory scan information and/or configuration files.

Name	Description
Change detection views	Configure Client inventory attributes to ...
Custom Views	Create unique folders and views of inven...
Inventory Views	View pre-defined Client inventory data

The following topics are included in this section:

- “Monitoring Inventory Changes”
- “Creating a New Folder in Custom Views” on page 455
- “Creating a Custom Inventory View” on page 455
- “Renaming a Folder or View” on page 456
- “Creating a Group within a View” on page 457
- “Viewing Client Type Inventory Data” on page 462
- “Acknowledging Monitored Inventory Changes” on page 462
- “Viewing a Specific Client’s Inventory Data”

Monitoring Inventory Changes

Fields to monitor

- Bluetooth
- Custom Data
- Device
 - Battery level (%)
 - Client date
 - Client name
 - Device OS
 - IMEI
 - OS version
 - Processor
 - Scan date
 - Serial number
 - User name

Condition: =
Value: 20

Notification method:
 Alert
 Visual
 Both

[Add](#)

Fields monitored

Schema	Class	Property	Notification method	Condition	Value
Windows...	Bluet...	Connec...	Visual	=	True
Windows...	Bluet...	Device ...	Visual	=	True
Windows...	System	ROM re...	Visual	=	5.2
Windows...	Device	Battery...	Visual	=	20

Condition: =
Value: 20

Notification method:
 Alert
 Visual
 Both

Delete

You must restart the service to use any new values.

OK Cancel

Using the Client type views in the Change detection views folder you can choose inventory attributes to monitor on the selected client type. Once set, you can view those clients that have detected inventory changes in the right pane of Inventory view and via the Clients view right pane shortcut menu.

To define attributes to monitor, right-click the Client type view, then choose **Configure change detection**. You can also click **Change detection** on the button bar.

In the Fields to monitor list, select an inventory attribute (field) to monitor for the selected client type.

If necessary, choose a condition (=, !=, <, >, >=, <=, and Like, if available) from the

Condition drop-down list.

Click the **Value** drop-down arrow to choose from a list of defined values, or enter the value in the field.

Select the type of notification(s) you want to receive when this attribute (field) changes on a client:

- **Alert** logs an alert to the server and displays the alert on Home, Alerts, and in the Raised Events view in Data views, Logs.
- **Visual** lists the client in Inventory view.
- **Both** generates both types of change notifications.

Click **Add** to include the attribute and its notification method in the Fields to monitor list. Once included, you can add or change the **Condition**, **Value**, and/or **Notification method** of an item by making your selections in the fields provided underneath the list.

To add more fields, repeat the information above.

To delete a selected field, click **Delete**.

Click **OK**. Inventory Manager monitors the fields listed and reports any clients that have changes in Inventory view.



You must stop and restart the Inventory Manager server service in order for change detection attributes to be enabled for monitoring.

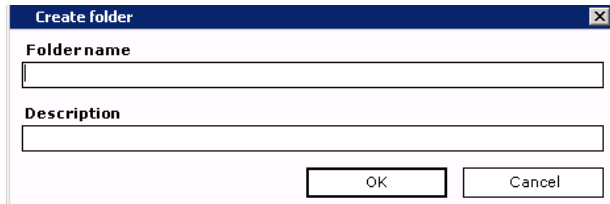


For details on stopping/starting the Inventory Manager server service, see "Stop Inventory Manager services" in the Inventory Manager chapter, *Afaria Reference Manual |Components*.

To view a client's reported changes and remove it from Inventory view, see "[Acknowledging Monitored Inventory Changes](#)" on page 462.

Creating a New Folder in Custom Views

You can create your own folders under the Custom Views folder. Right-click the **Custom Views** folder (or another custom folder under Custom Views), choose **New**, then **Folder** on the shortcut menu. The Create folder dialog box appears.



Enter a **Folder name** and **Description** for the new folder and then click **OK**. The folder is saved under the Custom Views folder in Inventory view.

Creating a Custom Inventory View

Create custom database views to return data from the database that is not already represented in a predefined view. You can create groups of related views within the Custom Views folder or another custom folder under Custom Views.



Custom views that you create are available for creating client groups. See [“Client Groups” on page 284](#).

To create a custom view, right-click the **Custom Views** folder and then choose **New, View**. The View editor dialog box appears in which you label and create/manage columns in the view.

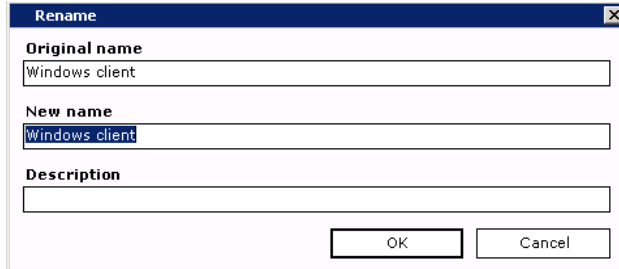
See also [“Creating Custom Database Views” on page 389](#) and [“Viewing a Custom View’s SQL Statement” on page 393](#).

Renaming a Folder or View



You cannot alter the name/description of predefined folders or views.

To alter the name and/or description of a folder or view, right-click the item and then choose **Rename** on the shortcut menu. The Rename dialog box displays the item's original name.



The screenshot shows a 'Rename' dialog box with the following fields and buttons:

- Original name:** Windows client
- New name:** Windows client
- Description:** (empty)
- Buttons:** OK, Cancel

Make alterations in the **New name** and/or **Description** fields, then click **OK**.

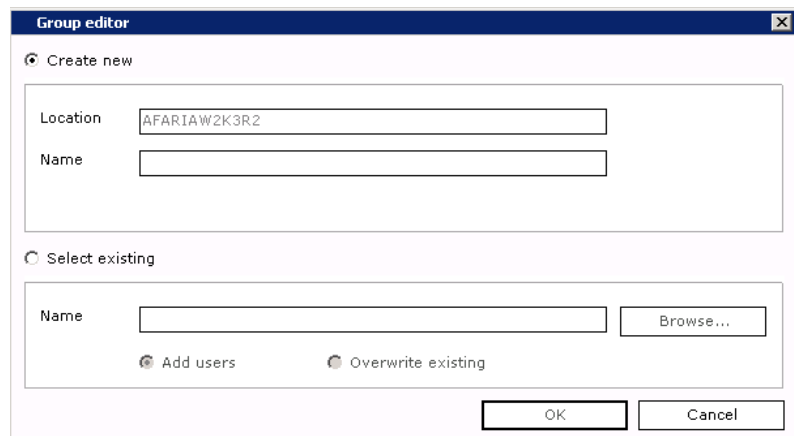
Creating a Group within a View

To create a group, right-click any view and then choose **New, Group** on the shortcut menu.

NT/LDAP groups

When you select **NT/LDAP** on the shortcut menu, the Group Editor dialog box for your server appears through which you can create new or select existing NT or LDAP groups. Once created, you can manage these groups through the operating system on which the server is installed.

NT



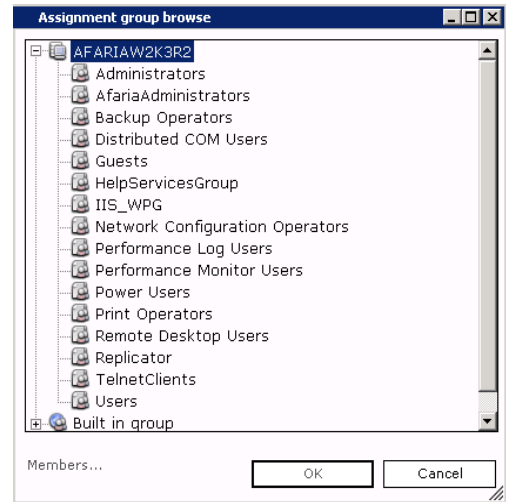
The screenshot shows the "Group editor" dialog box with the "Create new" radio button selected. The "Location" field contains "AFARIAW2K3R2" and the "Name" field is empty. The "Select existing" radio button is unselected. The "Name" field for the "Select existing" section is empty, and the "Browse..." button is visible. At the bottom, there are "Add users" and "Overwrite existing" checkboxes, both of which are unselected. The "OK" and "Cancel" buttons are at the bottom right.

Creating a new group is the default. **Location** defaults to the installed server. Enter the **Name** of the group.

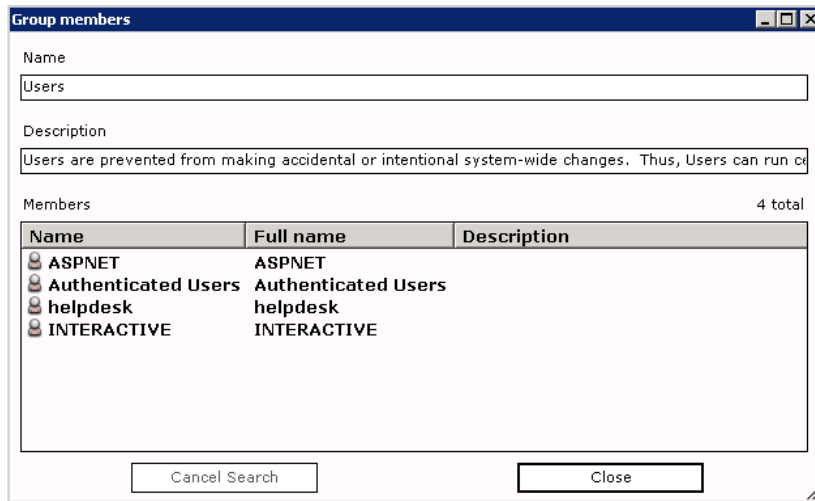
Local (default) allows you to create a group from specific NT user groups. **Global** allows you to create a group from the global NT domain.

To use an existing group, select the **Select Existing** radio button and then click **Browse**. The Assignment Group Browse dialog box appears. Expand the list to locate the group.

To view the members of a group, select it and then click **Members**.



Use the read-only Group members dialog box to view group information.

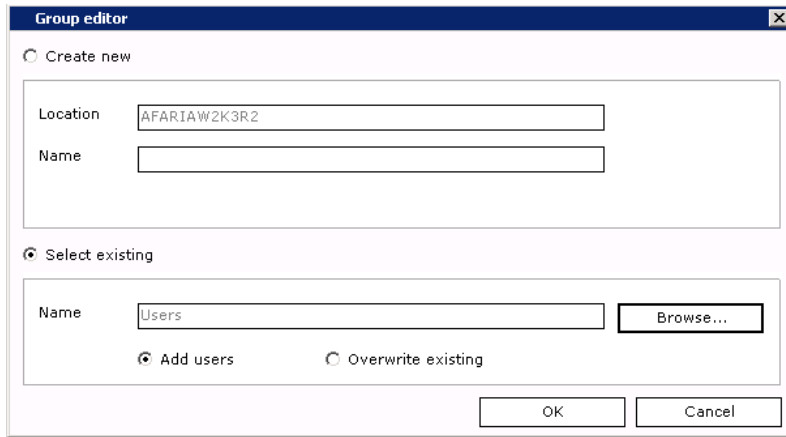


Name. Domain, or name of the group.

Description. Representation of the group, such as “Marketing.”

Members. The name, full name, and description of all group members.

Click **OK** to save the group name to the Name field in the Group Editor dialog box.



Group editor

Create new

Location: AFARIAW2K3R2

Name:

Select existing

Name: Users Browse...

Add users Overwrite existing

OK Cancel

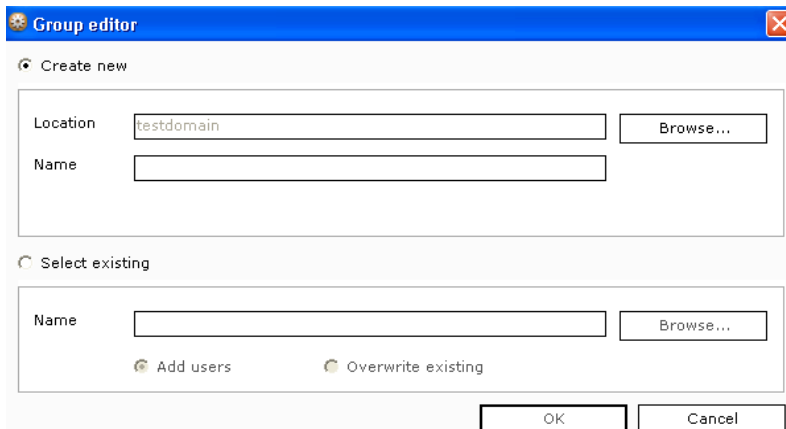
Click **OK** to close the Group Editor dialog box.



Clicking **OK** saves the new group to the operating system on which the server is installed, therefore the new group isn't visible in Clients view. Manage the group using the Administrative Tools provided by the operating system.

LDAP groups

Creating a new group is the default.



Group editor

Create new

Location: testdomain Browse...

Name:

Select existing

Name: Browse...

Add users Overwrite existing

OK Cancel

Location defaults to an organizational unit in the LDAP directory, but you can click **Browse** to select another group in the Assignment Group Browse dialog box.

Select a group and then click **OK** to return to the Group Editor dialog box.

Enter a **Name** for the group.

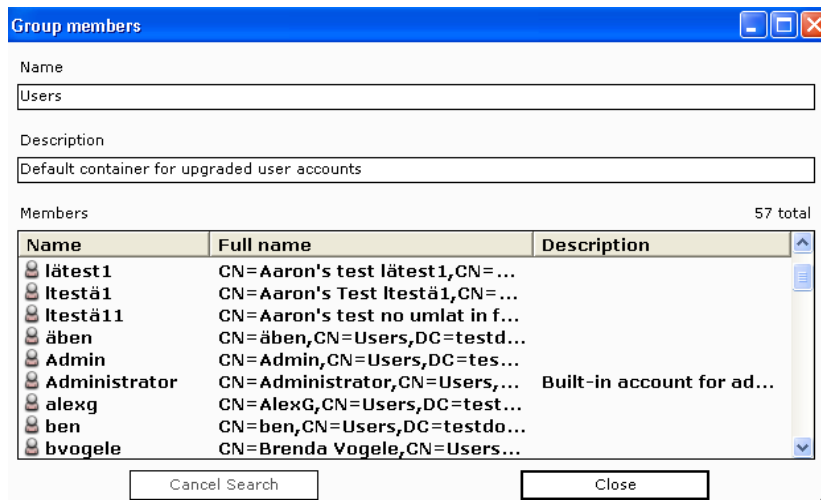
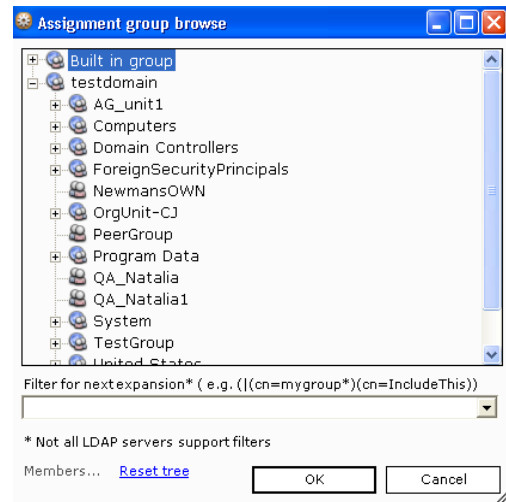
To use an existing group, select the **Select Existing** radio button and then click **Browse**. The Assignment Group Browse dialog box appears. Expand the list to locate the group.

To use a defined LDAP filter, enter it in the LDAP filter field.

To view the members of a group, select it and then click **Members**.

Use the read-only Group members dialog box to view all the members of the organizational unit you selected from the directory tree in the Assignment Group Browse dialog box.

LDAP servers place limits on how many entries you can view at once. If a group contains a large number of users, the list may be truncated by the LDAP server.

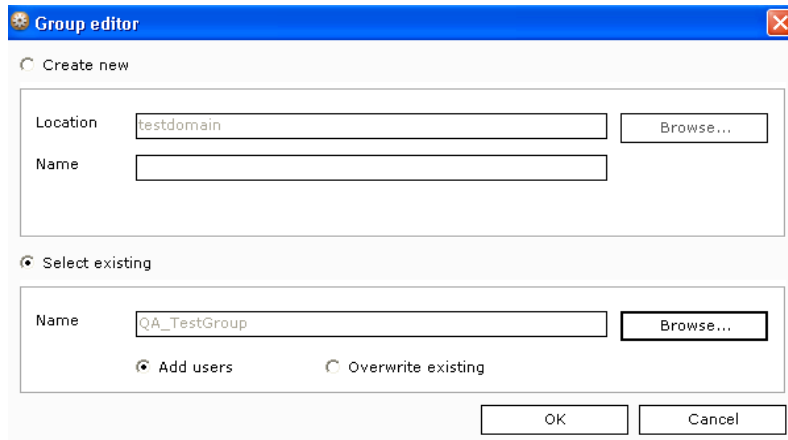


Name. Root to which the unit belongs, such as “mycompany.com.”

Description. Name of the organizational unit, such as “Human Resources.”

Members. The user’s name, full name, and description of all members of the selected group.

Click **OK** to save the group name to the **Name** field in the Group Editor dialog box.



The screenshot shows the 'Group editor' dialog box. It has a title bar with a close button. The dialog is split into two sections. The top section, 'Create new', has a 'Location' text box containing 'testdomain' and a 'Browse...' button to its right. Below that is a 'Name' text box. The bottom section, 'Select existing', has a 'Name' text box containing 'QA_TestGroup' and a 'Browse...' button to its right. Below the 'Name' field are two radio buttons: 'Add users' (which is selected) and 'Overwrite existing'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Click **OK** to close the Group Editor dialog box.



Clicking **OK** saves the new group to the operating system on which the server is installed, therefore the new group isn't visible in Clients view. Manage the group using the Administrative Tools provided by the operating system.

Dynamic client groups

When you select **Dynamic Client groups** on the shortcut menu, you can create new client groups.

Enter the name and description of your group and then click **OK**.

See "[Client Groups](#)" on page 284.

Viewing Client Type Inventory Data

When a client runs an inventory channel during a session, all scan results are transferred to the storage location you selected when you created the inventory channel, either a database used by the Afaria Server, an SMS Server, or both. You can view those scan results for all client types through the Inventory Views folder.

To view scan results, expand the client type (left pane) schema that you want to view and then select a class or property. The right pane displays its corresponding client inventory data in one or more columns.



Client value – For devices that do not return a client value as defined by Afaria, the value for client is the first 63 characters of the User value.


By default, Inventory Manager does not report software unless it's listed in the Software Catalog Editor. You can collect unlisted data; however, the length of the software inventory scan and the resulting data file size increases significantly, thereby increasing both time during communications sessions and database space requirements. For information about the Software Catalog Editor, see "Detection of software applications and operating system characteristics" in the Inventory Manager chapter, *Afaria Reference Manual | Components*.

For information on choosing a storage database, see "Set storage options" in the Inventory Manager chapter, *Afaria Reference Manual | Components*.

For details about using SMS with Inventory Manager, see "Route scan results to SMS database" in the Inventory Manager chapter, *Afaria Reference Manual | Components*.

For details on the inventory schemas, classes, and properties, see "Inventory schemas" in the Data views chapter, *Afaria Reference Manual | Components*.

Acknowledging Monitored Inventory Changes

When you define client inventory attributes to monitor via the Change Detection View folder, Select change detection attributes dialog box, the right pane displays all clients of the selected client type with detected changes. You can acknowledge a client's changes by right-clicking the Client row and choosing **Acknowledge changes**, or selecting the row and clicking  **Acknowledge change detection** on the button bar. You can also acknowledge changes via Data views, Clients.



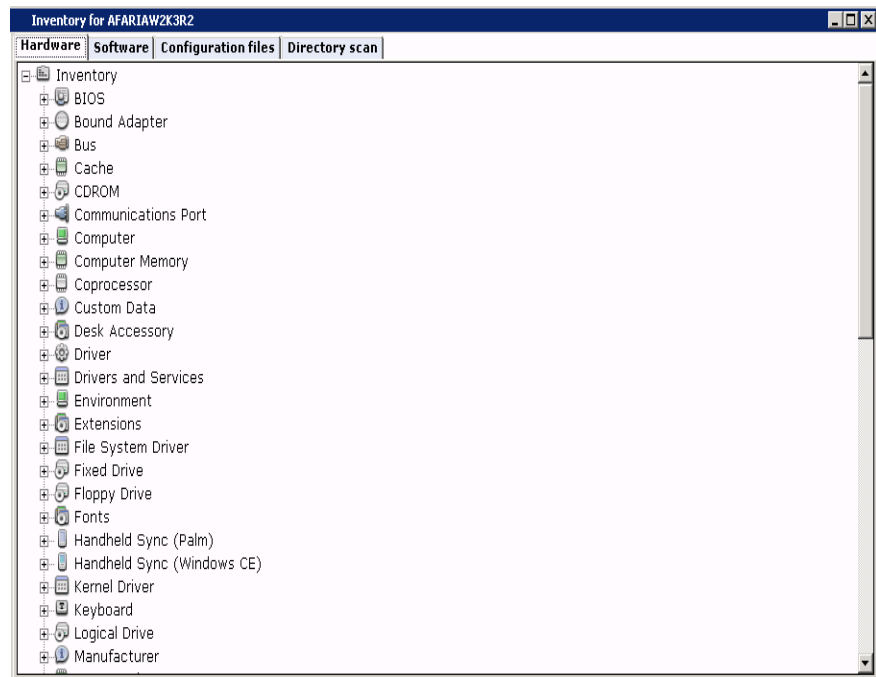
When a new client connects to the server, change detection values display "New." Inventory values are determined when a client connects rather than after the session completes.

The selected client is removed from the right pane.

Viewing a Specific Client's Inventory Data

You can view hardware and software inventory data for all clients, and for Windows clients you can also view directory scan data and configuration files. To access inventory data, expand the Inventory Views folder and select the client type to view. The right pane displays data specific to the selected view. Right-click a client row, then choose **Client inventory** to open the Client Hardware property page.

Hardware



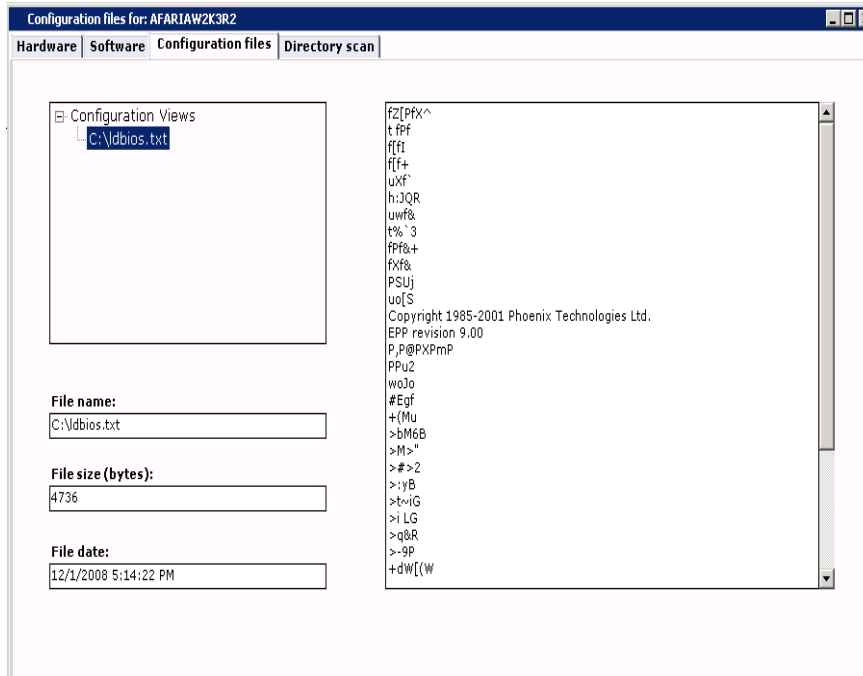
The Hardware property page lists the data that Inventory Manager collected and reported for the selected client. The data collected includes all of the classes and properties specific to the client type. You can view the classes and properties in the client specific folder. Hardware is collected for all client types.

Software

The Software property page lists the data that Inventory Manager collected and reported for the selected client. The data collected includes all of the classes and properties specific to the client type. You can view the classes and properties in the client specific folder. Software is collected for all client types.

Software for: AFARIAW2K3R2		
Hardware Software Configuration files Directory scan		
Name	Version	File date
Microsoft SQL	5.0.810.500	4/4/2003
Microsoft Corporation Installer for the Windows Installer	1.10.1029.1	4/4/2003
Microsoft Windows Installer	11.20.1827.0	7/27/200
Microsoft Windows Installer - Unicode	11.20.1827.0	7/27/200
Installer for the Windows Installer	1.20.1827.0	6/29/200
Microsoft Visual Studio .NET	7.10.3052.4	6/25/200
Sun Java	2.2.0.1621	4/8/2005
Sun Java	2.2.0.1621	4/8/2005
Microsoft Visual Studio .NET	7.10.3052.4	6/25/200
Afaria Server	6.00.4093.0	11/23/20
Microsoft Register Server	5.00.1586	1/1/1998
Afaria Client	6.00.4093.0	11/23/20
Intel Corporation Intel Windows USER	6.60.0.1	9/20/200
Inventory Scanner for Windows 95/NT	6.60.8.1	10/2/200
Microsoft Register Server	5.00.1586	1/1/1998
Platform Client	6.00.4093.0	11/23/20
Platform Client	6.00.4093.0	11/23/20
Platform Client	6.00.4093.0	11/23/20
Platform Client	6.00.4093.0	11/23/20
Platform Client	6.00.4093.0	11/23/20
Platform Client	6.00.4093.0	11/23/20
Platform Client	6.00.4093.0	11/23/20
Platform Client	6.00.4093.0	11/23/20
Intel Corporation Intel Windows USER	6.60.0.1	9/20/200
Inventory Scanner for Windows 95/NT	6.60.8.1	10/2/200
Microsoft Register Server	5.00.1586	1/1/1998
Afaria Client	6.00.4093.0	11/23/20

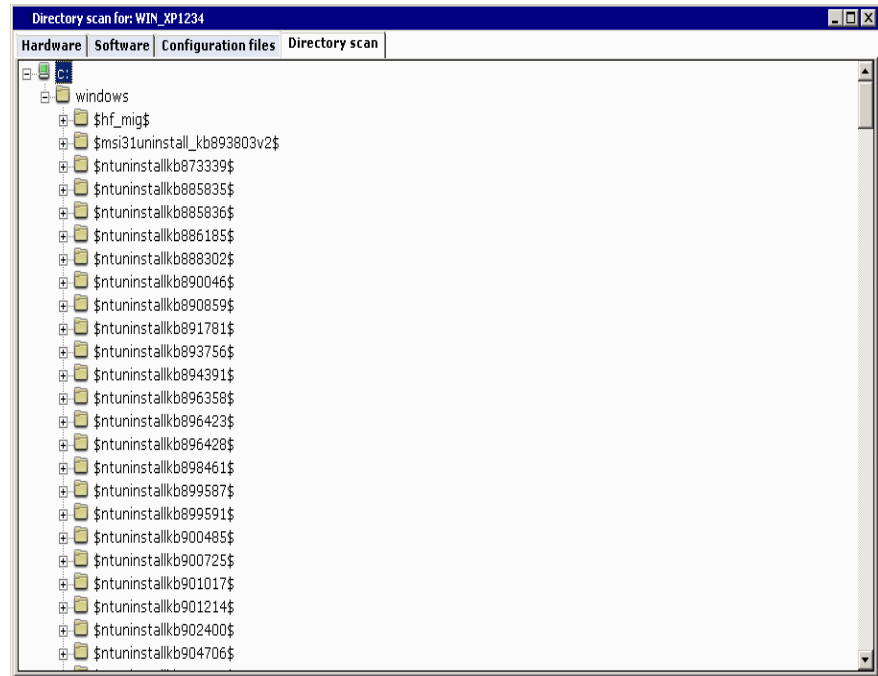
Configuration Files



You can view a Windows client's configuration files on the Configuration files property page. Select the file to view its contents. Information that appears includes the name of the configuration file, size of the file in bytes, time at which the file was last modified on the client, when the file was reported to the inventory database, and contents of the selected configuration file.

Directory Scan

When you define an Inventory Manager channel for Windows clients, you can optionally collect information on the directory and file structure of all local hard drives, or specific drives and paths at all of the clients that connect to the channel. If you choose to collect this information you can view it on the Directory scan property page.



For information on scan options at the Windows client, see "Set scan type" in the Inventory Manager chapter, *Afaria Reference Manual | Components*.

Track Software Manager channels

Package tracking view allows you to examine the delivery and installation status of your Software Manager channels at all clients, and for your Windows clients you can also view the status of an uninstall and/or cleanup. Using this information, you can ensure that your client users have the specific software they need to perform business-critical tasks. In addition, after a client connects to the server that sent the channel, data in Package tracking view is updated. Package tracking contains two panes:

- The left pane displays the folders and Software Manager channels available to your client users. Folders can represent the server from which the channel was deployed, as well as other folders. Channels display when a folder is expanded.



Right-clicking a channel displays a shortcut menu from which you can view the channel's properties.

- The right pane contains information specific to the item selected in the left pane. When a folder (Server) is selected, the software channel, description, and path display in column format. When a channel is selected, package tracking summary information displays.




Clicking a summary view displays the client name, client type, modification number, status, cleaned up status, and date/time in column format. Right-clicking a row displays a shortcut menu from which you can view status properties.

Software package	Description	Channel path
SWMgr		\AFARIAW2K3R2

The following topics are included in this section:

- “View package properties” on page 468
- “Work with software tracking views” on page 470
- “Display tracking status views” on page 471
- “View client status properties” on page 471
- “How package tracking works” on page 473

View package properties

You can view the properties of any channel by selecting it and then clicking  **Package properties** on the button bar, or right-clicking the channel and choosing **Package properties** on the shortcut menu.

The read-only Software package properties dialog box allows you to view the name and characteristics of the selected channel. Each Property description follows.

Channel path provides the exact location of the resource files from which the server deploys the channel.

Channel state displays Deleted, Published, or Unpublished.

Delivery model displays Delivery based when the channel is delivered to the handheld or Windows client; LAN based when the channel is installed at the Windows client from a LAN location.

Description (optional during channel creation) provides additional label information for the channel.

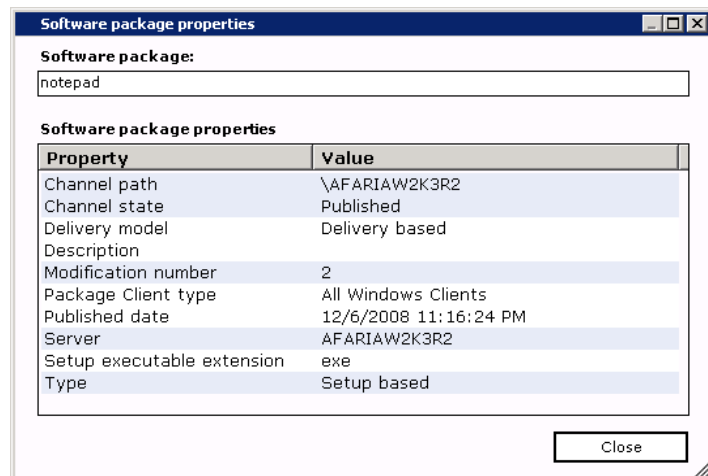
Modification number displays the current number of times that the channel has been significantly modified, requiring channel re-delivery.



The Modification number may be different in Clients view, Package tracking mini-view depending upon the state of the channel at the client.

The Modification number represents the SigVer.

Package Client type provides the device type for which this channel was created.



Published date provides the last date and time that the channel became available to clients. If the channel is unpublished, then no date displays.

Server provides the name of the computer that deploys the channel.

Setup executable extension displays a value if the channel is a Windows client setup based installation. The value that displays represents the type of setup program. Program types include .msi, .com, .exe, .bat, .zip, and others.

Type provides the method of channel installation, Setup or Non-Setup based.



For information on organizing source file for channel deployment, see “Organize channel creation and deployment” in the Software Manager chapter, *Afaria Reference Manual | Components*.

For information on delivery models and installation types, see “Create channels for Windows clients” in the Software Manager chapter, *Afaria Reference Manual | Components*.

Click **Close** to return to Package tracking view.

Work with software tracking views

When you select a channel to track in the left pane, the right pane displays a summary of client status information specific to that channel.

All Clients provides delivery/installation status for all clients.

Delivery status (started, partial, completed, failed) displays the clients that have attempted to receive the channel.

Installation status (started, completed, failed) displays the clients that have tried to install the channel.


Uninstall status (uninstalled, failed) displays the clients that have tried to uninstall the channel.

Package tracking views	Client status
All Clients	1 Clients
No Delivery attempted	0 Clients
Delivery started	0 Clients
Partially delivered	0 Clients
Delivery completed	1 Clients
Delivery failed	0 Clients
Installation started	0 Clients
Installation completed	0 Clients
Installation failed	0 Clients
Uninstalled	0 Clients
Uninstall failed	0 Clients

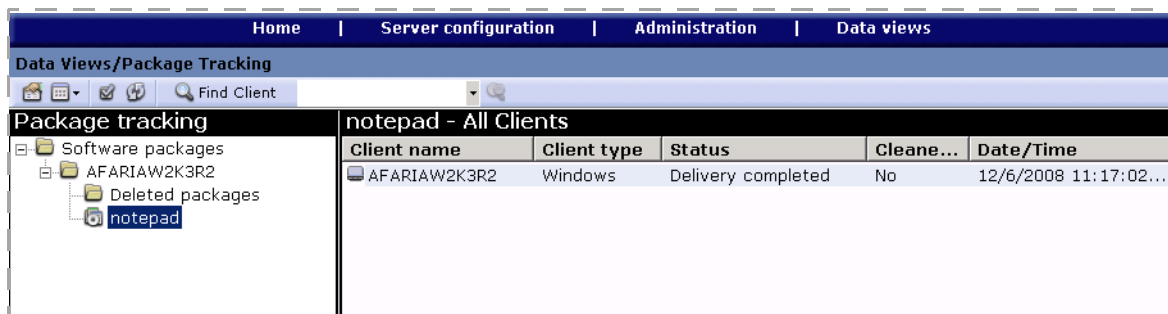


Not all channels report on all states.

Display tracking status views

You can display a view by clicking  **View** on the button bar and making your selection, or clicking a link in the summary.

Following is a portion of the All Clients view. Data displayed in column format includes the client name and type, number of modifications (representing the number when delivered at the client), status (each different status has a unique view listed under summary), whether a Windows client user performed a cleanup, and the date and time of the event in the Status column.



Client name	Client type	Status	Clean...	Date/Time
AFARIAW2K3R2	Windows	Delivery completed	No	12/6/2008 11:17:02...

Open a client's context menu and choose **Status properties** to view status properties.



For information about the Client status properties window, see ["View client status properties"](#).

View client status properties

You can view the status of a channel at the client by right-clicking the client row (in the right pane) and choosing **Status properties**. The properties include software channel details, typically including code, date, string, and/or SigVer (Significant Version number).



To understand how a SigVer works, see ["How status is determined"](#) on page 473.

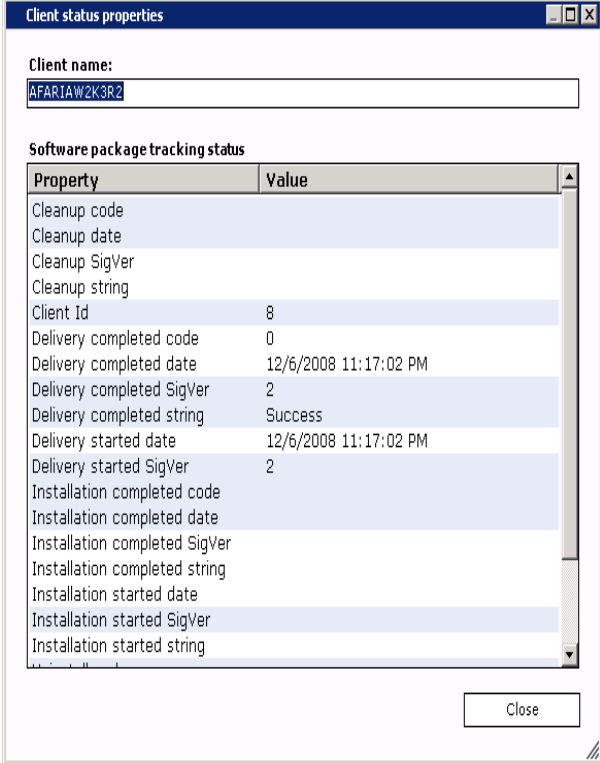
Code is a numeric indication of the success or failure of the action. Negative numbers indicate failure; non-negative numbers indicate success. For example, **0** indicates unconditional success, while **1** in the Delivery completed code might mean partial delivery of a segmented channel.

Date represents the date and time of the indicated action.

SigVer represents the channel version at the time and location of the action. It often displays as “Modification number.”

String is a readable indication of the state of the action, for example the percentage complete for delivery of a segmented channel would display in Delivery completed string.

Cleanup data displays if the channel was created for Windows clients and delivered to the client, rather than being deployed via a LAN location. It indicates that files stored temporarily in a location at the client (staging area) were removed.



Property	Value
Cleanup code	
Cleanup date	
Cleanup SigVer	
Cleanup string	
Client Id	8
Delivery completed code	0
Delivery completed date	12/6/2008 11:17:02 PM
Delivery completed SigVer	2
Delivery completed string	Success
Delivery started date	12/6/2008 11:17:02 PM
Delivery started SigVer	2
Installation completed code	
Installation completed date	
Installation completed SigVer	
Installation completed string	
Installation started date	
Installation started SigVer	
Installation started string	



For information about how the Windows client user performs a cleanup, see “How the Windows Client user cleans up installation files” in the Software Manager chapter, *Afaria Reference Manual | Components*.

Client ID represents the computer ID.

Delivery completed is updated every time the channel actually delivers content to the client. No value displays for Windows client LAN based installation channels.

Delivery started represents the last time that the channel was started. It displays no **code** or **string** because it's irrelevant to retrieve failure to start information. No value displays for Windows client LAN based installation channels.

Install completed represents installation complete on Windows client channels; after channel delivery on channels for Palm clients and Windows Mobile clients that don't include .cab files. No value displays for Windows Mobile channels that include .cab files unless a registry value is provided.



For information on setting installation options for Windows Mobile clients, see "Define installation at a Windows Mobile client" in the Software Manager chapter, *Afaria Reference Manual | Components*.

Install started represents channel installation started and progressed as far as starting the setup executable on Windows client channels; after channel delivery on channels for Palm clients and channels for Windows Mobile clients defined with automatic installation or that don't include .cab files. No value displays for Windows Mobile client channels that include .cab files or that aren't defined to install automatically.

Uninstall represents that the channel was uninstalled.

How package tracking works

Each time a client connects to the server, that client's computer identification number and computer name are reported to the server's database and disbursed to tables that need that data. One of the tables that needs that information is Client Package Status, discussed below.

Another Afaria Server database table, Packages, collects data about each software channel on the server. Important data collected includes the original channel and server identification numbers, which when uniquely paired together allow centralized databases for an entire company, rather than for a local server. It also works in replicated channels, long distance and on server farms. The unique pair collected in the Packages table is also reported to the Client Package Status table.

At this point, the Client Package Status table has not only received the client's computer identification number, but also the unique pair. This table combines the information to create a unique key for each row for each client that connects to each channel. Simply stated, the number of table rows equals the number of software channels multiplied by the number of clients.

How status is determined

The key to determining the status of a software channel is the Significant Version number (SigVer), which is maintained by the channel. Every time a channel modification requires a client that has already installed the channel to reinstall the channel, the SigVer increases. The SigVer appears in both the Client Package Status and Packages tables.

The SigVer that's stored in the Packages table represents the current SigVer for the channel. It's used to determine the SigVer of the channel that exists at the client. For example, if a channel delivered to a client is SigVer 5 and the current channel SigVer is 6, then the client hasn't taken delivery of the most recent channel version.



Some channel modifications don't change the SigVer and therefore don't require a reinstall. Modifications of this sort include changing the administrator defined version of the channel, which doesn't change binary files sent to the client. However, changing a size or time stamp in one of the channel files would cause a change to the SigVer.



Data collected in the Client Package Status table displays in the Client status properties dialog box. For information about the data that displays in this dialog box, see ["View client status properties" on page 471](#).

How Package tracking view displays deleted software channels

When you publish a software channel in Administration > Channel Administration, Package tracking view creates a folder to represent the server on which the channel was created and places the published channel in that folder. If you delete a published channel in Channel Administration, Package tracking view creates a "Deleted packages" folder under the Server folder. The deleted channel remains in that folder but returns no status information. You can remove the channel from the Deleted packages folder by right-clicking it and choosing **Delete package** on the shortcut menu.



When you delete a client via the right pane in Clients view, all rows detailing the status of channels on that client are deleted. If you create a new client using an old computer name, then Package tracking view prompts you to either keep both copies of the client or delete the older one(s). If you choose to keep both copies of the client because a hard disk is being replaced or reformatted, then the new client gets a new unique identifier and reappear in the Client Package Status table.

Keeping multiple copies of a client can create misleading "old" information. In the case of the WAN with multiple Domain Name Servers, it's possible to have multiple computers active with the same name. However, deleting the old client ensures a cohesive WAN where computer names are unique and collisions are fixed, as well as a WAN with several separate name spaces for LAN names.

For information on deleting a client in Clients view, see ["Deleting Client Data" on page 412](#).

How actions happen

Actions happen in a particular order. The order of actions and the SigVers present represent the status of a particular client. Delivery happens before installation can begin, which happens before installation can end, which happens before uninstallation. Cleanup can happen any time after delivery, but only on delivery based channels created for Windows clients. If two actions have the same SigVer, then the time stamp indicates which of them actually happened last.

Example 1

If a Windows client channel has SigVer 6 and the Client status properties dialog box indicates Delivery completed SigVer 5, Installation completed SigVer 3, and no uninstall or cleanup information, then an old version is installed and delivery has been taken on a newer version even though no action has occurred.

Example 2

If a Windows client channel, Client status properties dialog box indicates Delivery completed, Installation started, Installation completed, Uninstalled, and Cleanup SigVer 6, then the channel was delivered, installed, uninstalled, and cleaned at least once. Therefore, if the time stamps indicate that the last action that occurred was installation, then the channel is currently installed.

Example 3

If the channel SigVer is 5 and the Client status properties dialog box indicates Delivery completed SigVer 5, Installation completed SigVer 4, and Installation completed code Success, then the client user has installed some version of the channel and is attempting to install the current version.



The Client Package Status table is updated on the next connection to the server after an action occurs on the Client. Updates to the Packages table, as well as to the Delivery started date and SigVer are reflected immediately.

Restore backed up client data

Backup view displays the files/folders that have been backed up from your clients via Backup Manager channels. Using this view you can examine the relationship between clients, their backed up data, and their associated hardware. You can restore items to those clients, and if necessary copy/paste items from one client to another of the same client type. You can also delete at one time all backed up items older than a defined number of days.



You can view Backup Manager channel activity in Logs view: Messages, Sessions, and File transfers folders. Windows client users can view the Session Log Control in Channel Viewer. Handheld client users can view backed up items by pressing the Log button on their devices.

Backup view contains two panes:

- The left pane may display icons that represent servers, computers, disks, folders, and files.



Right-clicking an icon other than the server displays a shortcut menu from which you can cut, copy, paste, delete, restore and cancel the restoration of items.

- The right pane displays the name, size, type, and modification date of the item selected in the left pane.



Right-clicking an item in the right pane displays a shortcut menu from which you can delete, restore and cancel the restoration of the item.

The screenshot shows the Backup Manager interface with the following components:

- Navigation tabs: Home, Server configuration, Administration, Data views.
- Page title: Data Views/Back-Up.
- Toolbar: Includes icons for backup, restore, delete, and search, along with a "Find Client" search box.
- Left pane (Backup): Shows a tree view with "Backup data" expanded to show "ENGWIN2K3VM" and its sub-folder "c".
- Right pane (C): A table listing backed up files.

Name	Size	Type	Modified
<input type="checkbox"/> Monthly Leave.doc	82 KB	File	11/25/2008 6:13 PM
<input type="checkbox"/> SVCSFlowOP1.doc	49 KB	File	11/25/2008 6:14 PM
<input type="checkbox"/> Tasklist Project Wrapup.doc	194 KB	File	11/25/2008 6:14 PM

Current view: Clients (1 Row(s)) More data

The following topics are included in this section:

- [“How hardware and backed up data are represented”](#)
- [“How clients are represented” on page 479](#)
- [“Clean up backed up items” on page 481](#)
- [“Selectively restore items to clients” on page 481](#)

How hardware and backed up data are represented

The following icons may appear in the left pane of Backup view.



Server is the starting point of contact in the system. It contains a hierarchical collection of channels and folders. Clients connect to a server to access its channels.



Single computer represents one computer or the unique computer identifier when there are multiple computers with the same name.



Grouped computers represent more than one computer, all with the same computer name.



Grayed out single computer represents an item that has been cut, and will remain in this state until pasted into another location.



Disk represents a drive.



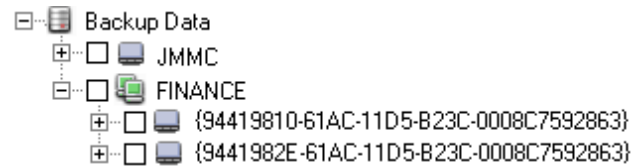
Folder represents a folder.



File represents a file.

How clients are represented

When a Backup Manager channel backs up data at a client with a unique computer name, Backup view displays a single client computer under the server's backup location. Notice "JMMC" in the illustration at right.

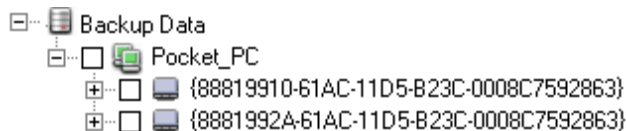


When items are backed up on clients that share the same computer name, such as "FINANCE" in the illustration, then the group computer icon appears. Expanding the group computer icon displays its individual computers as unique identifiers, rather than as separate computers "FINANCE01" and "FINANCE02" under the server's backup location. The data backed up in those unique identifiers is dependent upon the Backup Manager channels that executed on those computers.

You can cut, copy, paste, and delete content at the single computer and unique identifier level.



If you perform a hard reset on an un-serialized handheld client, then a separate unique identifier is created under the client's name, but only if the client name remains the same after the hard reset. Notice the illustration below.



You can learn more about how the client identifier is created at ["About the Afaria client identifier" on page 48](#). You can learn about how to merge separate client histories that belong to a single device at ["Combining a Client's Afaria Client ID" on page 413](#).

If you expand the tree node to view a specific client's data, then receive the "Unable to access Client data" Message box, the expand/collapse icon disappears. Possible reasons for receiving this message include a change in the backup location; a GUID deleted through Windows Explorer; a network problem and the location is inaccessible, such as a computer is down; or a network permission problem. The message only appears once per client, unless you refresh the view. If this message appears on multiple clients, then there may be a systemic problem rather than a problem with a specific client's data.

Work with backed up items

To manage backed up client data, expand the client that contains the data to manage and then using the button bar or shortcut menu, perform one or more of the following functions:

- **Save** stores all unsaved actions. Selecting another client or exiting Backup view also saves changes.
- **Cut** duplicates a selected item on the Clipboard and then removes it from the list.
- **Copy** duplicates a selected item on the Clipboard.
- **Paste** inserts a previously copied item below the currently selected item.
- **Delete** permanently removes the selected item from the list. The software prompts you to confirm deletion.

Select the filename(s), click Delete and then respond to the prompt.

To delete multiple files in the left or right pane, select each file, not the file's check box.

To delete a group of files, select the first file, hold down the Shift key and then select the last file.

To select multiple non-contiguous files, hold down the Control key.

If selecting multiple filenames does not leave focus on the file you're selecting, click the file's icon instead of the file's name.

- **Restore** marks the selected item to be restored to the device. (The check box to the left of the item is only for Restore.)
- **Cancel** restore removes the item marked from the restore process.
- **Refresh** displays updated information in the Backup view.



Windows client users should empty their Recycle Bin before running a Backup channel defined to back up all files of a specific type, including those within subfolders. Backup Manager executes these channels by retrieving the file type specified from the Recycle Bin, if any exist, and displaying them in the Back up view under the client in a "Recycled" folder. Files retrieved from the Recycle Bin are renamed according to Microsoft's naming conventions, as in "Sales.txt" to "DC11.txt." The Recycle Bin does not allow files to be copied into it, therefore we do not restore files from the Recycled folder. Recycled folders that appear in the Back up view have no benefit and can be deleted.

After running a Restore channel, click Refresh to see the effects of the channel. If the check boxes next to the items marked for restore are still selected, then the Restore channel didn't run properly. Clear all of the items' check boxes, then re-run the Backup channel for those items.

Data backed up from handheld devices can be restored to those devices through their respective desktop synchronization software. Device data stored in the Back up view can be used to restore companion PCs that have failed.

Changes made to clients that have been backed up need to be performed in the Back up view. Making any modification through Windows Explorer can cause unpredictable results.

Selectively restore items to clients

Backup view allows you to choose the clients and files/folders to be restored. In the left pane, select the clients to receive the backed up items. The right pane displays the files/folders available. Select the items to restore, then click the **Save** button.




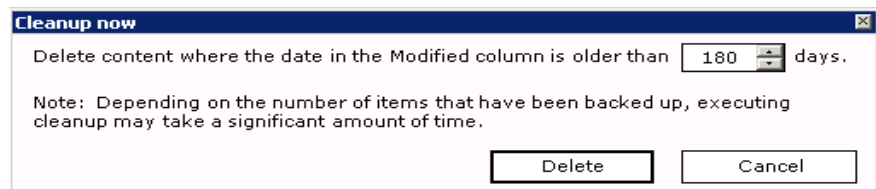
In a Selective Restore channel, once a selected client(s) successfully receive(s) the restored files and folders, the ability for the client(s) to re-connect to the channel to re-receive and re-restore the items will be prohibited. To allow the client(s) to re-restore previously restored items you must re-select them in the right pane of the Backup view.

After running a Restore channel, you must perform a Refresh to view the effects of the channel. You can refresh the view by clicking the **Refresh** button or leaving and then returning to Backup view. If performing a Refresh still displays selected check boxes next to the items marked for restore, then the Restore channel didn't run properly. You must clear all of the items' check boxes in order to re-run a Backup channel on the those items.

Clean up backed up items

You can define a specific number of days when all backed up items are deleted. The date on which deletion will occur is the defined number of days after the date that appears in the Modified column in the right pane of Back up view.

To set the date on which backed up items will be deleted, click  **Cleanup** on the button bar. The Cleanup now dialog box appears.



Enter or use the spin buttons to define the days after the last modification date when all backed up items will be deleted. The value must be greater than 0.



The value that you enter will not be retained. After the cleanup is performed, the value returns to its default, 180.

Depending upon the number of items that are backed up, cleanup may take a significant amount of time.

Click **Delete**. The cleanup is performed immediately and the dialog box closes.

Tracking Software Compliance and Usage Data

License compliance view allows you to examine software license compliance and usage data collected via Inventory Manager scans.



You must have at least *Read* permission in Access policies in order to access this link.

License compliance view contains two panes:

- The left pane displays two folders. The License Compliance Views folder contains predefined views for client types for each category of client. You can use these views to collect data, or you can define your own folders and views within the Custom Views folder.



Right-clicking an item displays a shortcut menu. Depending upon the selected item you can create new folders and views; cut, copy, paste, delete, and/or rename; edit a view; and view item properties.

- The right pane displays data, in column format, specific to the item selected in the left pane.



Selecting an item in the left pane runs a query on the item's properties, then displays view-specific data in column format in the right pane. You can also double-click the item in the left pane to display its content in the right pane.

Name	Description
Custom Views	Create unique folders and views of license compliance data
License Compliance Views	View predefined license compliance data

The following topics are included in this section:

- [“Working with Predefined Views”](#)
- [“Creating a Folder” on page 484](#)
- [“Create a Custom License Compliance View” on page 485](#)
- [“Viewing License Compliance Log Entries” on page 486](#)

Working with Predefined Views

When you select the License Compliance Views folder in the left pane, the right pane displays license data summary for the client sub-folders. Whereas, when you select a client folder in the left pane, the right pane displays data specific to that client category.



Size and usage data are not shown in summary view.

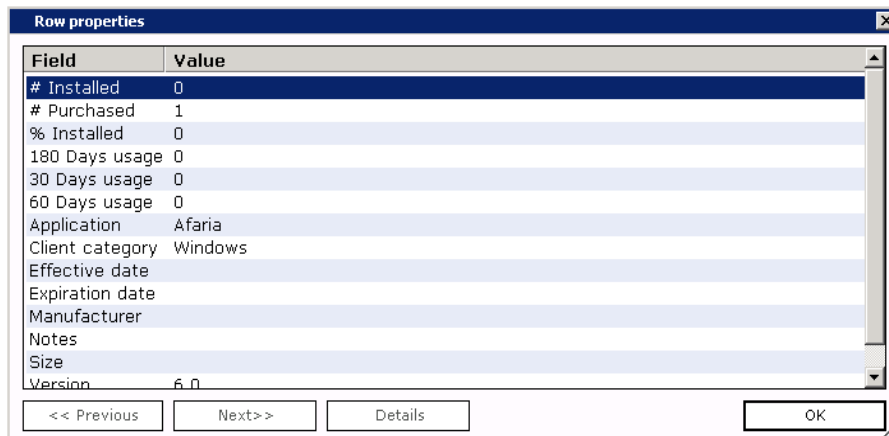
To change the sort order of a column, click its header; to change the order in which data displays, drag a column header to a new location.

The screenshot shows the Afaria software interface. The top navigation bar includes 'Home', 'Server configuration', 'Administration', and 'Data views'. The main window is titled 'Data Views/LicenseCompliance'. The left pane shows a tree view under 'License compliance' with folders for 'Custom Views', 'Client software installation', and 'License Compliance Views'. Under 'License Compliance Views', there are sub-folders for 'BlackBerry', 'Palm', 'Symbian', 'Windows' (which is selected), 'Windows Mobile Professional', and 'Windows Mobile Standard'. The right pane displays a table with the following data:

Client category	Manufacturer	Application	Version	# Purch
Windows		Afaria	6.0	1

View row detail

You can view detail of a specific license record in the Row properties dialog box by double-clicking the row that contains the record you want to view. You can also right-click the row and choose **Properties** on the shortcut menu.



Depending upon the client category, some fields will not contain data. For example, version data is unavailable for Symbian and BlackBerry clients; size data is unavailable for Windows and Windows Mobile Professional clients.


Click **Previous** or **Next** to view properties for other records.

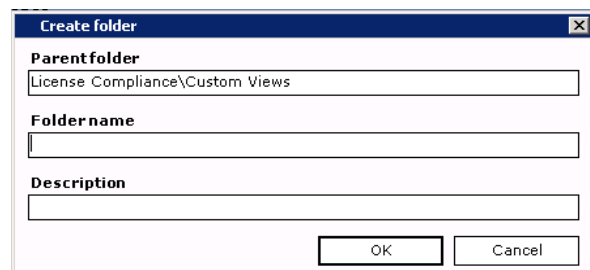
If Notes have been entered about a specific field, click the **Details** button to view the information in the Item details dialog box.

Click **OK** to return to the Row properties dialog box.

Click **OK** again to return to Data views, License compliance.

Creating a Folder

You can “nest” folders within the Custom Views folder to create a hierarchical structure. Select the parent folder, click  **New**, then select **Folder**. The Create folder dialog box appears.




In the Create folder dialog box, the read-only Parent folder field displays the intended location for the new folder. Enter a **Folder name** and **Description** and then click **OK**. The folder is saved under the parent folder.



If you want to change the location of the new folder, you must close the Create folder dialog box and select another parent folder.

Create a Custom License Compliance View

Create custom database views to return data from the database that is not already represented in a predefined view. To create a new view, select the Custom Views folder—or a folder within that folder—click  **New**, then select **View**. The View editor dialog box appears in which you label and create/manage view columns.

See also [“Creating Custom Database Views” on page 389](#) and [“Viewing a Custom View's SQL Statement” on page 393](#).

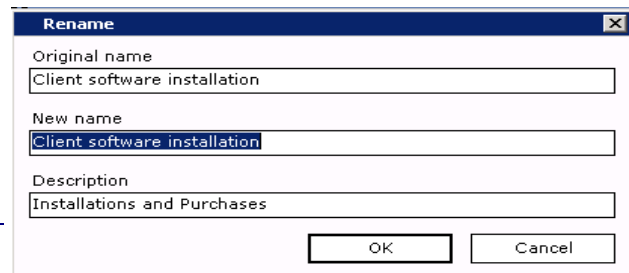
Renaming a View

To alter the name and/or description of a view, right-click the item and then choose **Rename** on the shortcut menu. The Rename dialog box displays the item's original name.

Make alterations in the **New name** and/or **Description** fields, then click **OK**.




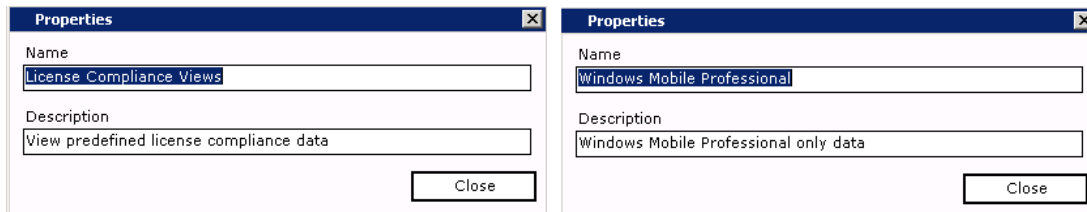
You cannot alter the name/description of predefined folders or views.



Rename	
Original name	Client software installation
New name	Client software installation
Description	Installations and Purchases
OK Cancel	

Viewing Folder or View Properties

You can view the properties of a selected folder or view by clicking  **Properties** on the button bar or right-clicking the item and choosing **Properties** on the shortcut menu. The dialog box left and below represents a folder's properties, while below right represents a view's.



Viewing License Compliance Log Entries

You can examine occurrences of any license compliance action that affected the server in the Data views, Logs, Messages folder. License compliance-specific messages are prefixed by LCU and appear when license definitions are created, copied, edited, deleted, or have a name change. LCU messages also appear when the scheduler begins, completes, or skips a license compliance refresh. The scheduler also displays messages (XRS) when it begins and completes a license compliance refresh. Data views generates license compliance when custom views are created, modified, and deleted. These messages are prefixed by DWS. All license compliance messages are information based and all indicate whether the action performed was successful or unsuccessful.

Date/Time	Server	Server user	Type
12/5/2008 5:19:51 PM	AFARIAW2K3R2	AFARIAW2K3R2\Administrator	INFO
12/5/2008 5:13:53 PM	AFARIAW2K3R2	Administrator	ERROF
12/5/2008 5:13:52 PM	AFARIAW2K3R2	Administrator	ERROF
12/5/2008 5:13:51 PM	AFARIAW2K3R2	Administrator	ERROF
12/5/2008 5:13:50 PM	AFARIAW2K3R2	Administrator	ERROF
12/5/2008 5:03:34 PM	AFARIAW2K3R2	AFARIAW2K3R2\Administrator	INFO
12/5/2008 4:53:29 PM	AFARIAW2K3R2	Administrator	ERROF
12/5/2008 4:53:28 PM	AFARIAW2K3R2	Administrator	ERROF
12/5/2008 4:53:27 PM	AFARIAW2K3R2	Administrator	ERROF
12/5/2008 4:53:26 PM	AFARIAW2K3R2	Administrator	ERROF
12/5/2008 4:44:27 PM	AFARIAW2K3R2	AFARIAW2K3R2\Administrator	INFO
12/5/2008 4:38:53 PM	AFARIAW2K3R2	Administrator	USER
12/5/2008 4:38:51 PM	AFARIAW2K3R2	Administrator	INFO
12/5/2008 4:38:50 PM	AFARIAW2K3R2	Administrator	INFO
12/5/2008 4:38:40 PM	AFARIAW2K3R2	AFARIAW2K3R2\Administrator	INFO
12/5/2008 4:38:40 PM	AFARIAW2K3R2	AFARIAW2K3R2\Administrator	INFO
12/5/2008 4:38:40 PM	AFARIAW2K3R2	AFARIAW2K3R2\Administrator	INFO

See also [“Working with Logged Actions”](#) on page 439.

Viewing client patch information

The Client patches view provides a powerful query tool to help you learn about which Microsoft patches and service packs your clients have installed and which they are missing. It also provides a powerful action tool to allow you to react quickly to security risks.

The view is filtered to include only the current patch selection you have in the Server configuration Patch console page, rather than all possible Microsoft patches identified in the Patch console page, and the current information that the server has collected from clients.



The Client Patch view requires that you have prepared the patch list in the Patch console for first-time use. Client data populates the view after clients connect and run a Patch Manager channel. See [“Patch console” on page 212](#).

The screenshot shows the 'Data Views/ClientPatchView' interface. On the left is a tree view of 'Client patch view' with sub-items like 'Clients', 'AGXPSP3', 'WIN_XP1234', 'Client groups', 'Sales SW All', 'Sales NW All', 'Div1_Dev', 'Div1_Doc', 'WM-Professional - S', and 'aaa'. The main area displays a table titled 'WIN_XP1234 - Missing patches' with columns: Update ID, Client, IsDownlo..., Title, and Product. Below the table is a section 'Clients Missing Selected Patches' listing 'WIN_XP1234'. At the bottom, it says 'Current view: WIN_XP1234 (20 Row(s))' and has a 'More data' button.

Update ID	Client	IsDownlo...	Title	Product
530603	WIN_XP1234	No	Cumulative Security Update for Outlook Express for Win...	Window:
530829	WIN_XP1234	No	Security Update for Windows XP (KB935840)	Window:
531643	WIN_XP1234	No	Security Update for Windows XP (KB935839)	Window:
672040	WIN_XP1234	No	Security Update for Windows Media Player 9 (KB936782)	Window:
674391	WIN_XP1234	No	Security Update for Windows XP (KB938127)	Window:
785699	WIN_XP1234	No	Security Update for Windows XP (KB933729)	Window:
861806	WIN_XP1234	No	Security Update for Windows XP (KB943460)	Window:
886729	WIN_XP1234	No	Security Update for Windows XP (KB944653)	Window:
887871	WIN_XP1234	No	Security Update for Windows XP (KB937894)	Window:
952269	WIN_XP1234	No	Security Update for Windows XP (KB943485)	Window:



Afaria’s ability to detect whether a patch is installed on a client is subject to Microsoft’s implementation for installing and removing patches. Therefore, the Client patch view may continue to show a patch as installed, after it is removed from the client using the client’s Add/Remove Programs feature. It may also continue to show an installed patch as missing.

The shortcut menu includes the following query and action selections when you select patches from the top right pane:

- Action – Create a static client group for selected clients that are missing a selection of patches.
- Action – Create a dynamic client group for all clients that are missing a selection of patches.
- Action – Create an unpublished Patch Manager channel for all clients that are missing a selection of patches.

- Action – Download a selection of patches.

See *Afaria Reference Manual | Components*, Patch Manager, for additional information on using the Patch Manager component.

Making a query

Using the Client patches view begins with making a default query. The default is a query that uses the “missing patches” filter. This query returns all the clients that are missing patches, based on the current patches you have selected in the Server configuration Patch console page. You can change the filter for any query, but this default filter is restored each time you change your client or client group selection.

To make a query:

- 1 On the global navigation bar, click **Data views** and then select **Client patches** on the drop-down menu. The Data views, Client patches page appears.
- 2 Select any client or client group in the left pane to display results for only that client or client group. Client group information includes information for all clients in the group.



- 3 Use the toolbar's **Filter** icon to choose a new filter, according to the following values:
 - All patches – Show patches that are installed and not installed on clients, without service pack information.
 - Installed patches – Show only patches that are installed on clients, without service pack information.
 - Missing patches – Default filter. Show only patches that are not installed on clients, without service pack information.
 - Installed Service Packs – Show only service packs that are installed on clients, without patch information.

Results display in the top right pane. You can click a column heading to sort by a column's values, or click and drag column headings to rearrange column order.

Creating a static client group for clients missing patches

You can use the Client patches view to create a static client group made up of a selection of clients missing one or more specific patches.

Using groups may help you to simplify Patch Manager channel management. See [“Client Groups” on page 284](#).

To create the group:

- 1 Make a query, as described in [“Making a query” on page 488](#).
- 2 Select one or more patches in the upper right pane. If any of your Patch Manager clients are missing any of the selected patches, those clients populate the Clients Missing Selected Patches pane in the lower right area of the window.
- 3 Select one or more of the clients for the group from the Clients Missing Selected Patches pane in the lower right area of the window.
- 4 Open the shortcut menu and select **Create Static Client Group for Selected Clients** to open the Create Client Group dialog.
- 5 Type a client group name and click **OK**. This group name is not validated against existing group names. Take care to avoid duplication.

The new static client group appears on the Client patches page populated with the clients you selected.

Creating a dynamic client group for clients missing patches

You can use the Client patches view to create a dynamic client group made up of all clients missing one or more specific patches.

Using groups may help you to simplify Patch Manager channel management. See [“Client Groups” on page 284](#).

To create the group:

- 1 Make a query, as described in [“Making a query” on page 488](#).
- 2 Select one or more patches.
- 3 Open the shortcut menu and select **Create Dynamic Client Group for Missing Selected Patches** to open the Create Client Group dialog box.
- 4 Type a client group name and click **OK**. This group name is not validated against existing group names. Take care to avoid duplication.

The new dynamic client group appears on the Client patches page populated with the appropriate clients.

Creating a channel for clients missing specific patches

You can use the Client patches view to create an unpublished Patch Manager channel to capture all clients that are missing one or more specific patches. You can choose to store channels anywhere in your existing channel folder structure, so you may want to create a specific folder structure or properties for this or future Patch Manager channels before completing this task.

Creating a channel launches the download process for any patches that are not already downloaded.

To create the channel:

- 1 Make a query, as described in [“Making a query” on page 488](#).
- 2 Select one or more patches.
- 3 Open the shortcut menu and choose **Create Channel to Deploy Missing Selected Patches** to open the Create Channel dialog box.



This new channel action applies only to the patches that are currently selected in the top right pane, regardless of the patches currently displaying in the bottom right pane.

- 4 Complete the Create Channel dialog box and click **OK**. You may be prompted with EULA dialogs. The Create Channel dialog includes the following data elements:
 - Channel name – A unique channel name. Use the channel directory tree to navigate your channel to an appropriate location.
 - Group name – Optional. A unique group name to create a dynamic client group to include any client that is missing one or more of the selected patches.
 - Profile Name – Optional. A unique group profile name to associate with the new channel.

Afaria executes the following actions based on your data:

- Creates a new, unpublished channel that appears on the Channel Administration page.
- If you named a new group profile name, Afaria creates a new profile with the new channel added to the allowed channels list.
- If you named a group, new dynamic client group appears on the Client patches page populated with the appropriate clients. The group is also assigned to the new profile if a profile was specified.

See [“Managing Profiles” on page 225](#) for additional information about further managing profiles.

Downloading patches on demand

You can use the Client patches view to download one or more selected patches.



Downloading patches is a resource-intensive process and can be lengthy.

- 1 Make a query, as described in [“Making a query” on page 488](#).
- 2 Select one or more patches.
- 3 Open the shortcut menu and choose **Download the Selected Patches** to launch the synchronization process, and then the download process for any patches in the selection that are not already downloaded. You may be prompted with EULA dialogs.

Consult the Messages log for download details.

View client deployment information

Client deployment view allows you to view information about client deployment notification messages processed from the client deployment center. Client deployment view contains two panes:

- The left pane displays the predefined client deployment folder.



Right-clicking an item displays a shortcut menu where you can view item properties or row count information.

- The right pane displays data specific to the item selected in the left pane.



When a view is selected, right-clicking a row displays a shortcut menu from which you can delete the item, display row properties, and view batch notification data.

Data Views/Client Deployment			
Client Deployment		Notification batches	
	Batch Name	Batch Description	Created
Client deployment views	Test template	Used by IT for testing	12/8/2008 10:41:
Notification batches	Notifications for executives	Standard notification sent to the members of the Executive group	12/8/2008 10:40:
Notifications	Notifications for executives	Standard notification sent to the members of the Executive group	12/8/2008 10:48:
Uncompleted notifica	Notifications for executives	Standard notification sent to the members of the Executive group	12/8/2008 10:49:
	Afaria client deployment notification	Standard notification for updated Afaria clients	12/8/2008 10:48:
	Afaria client deployment notification	Standard notification for updated Afaria clients	12/8/2008 10:38:
			12/8/2008 10:15:
			12/8/2008 10:43:
			12/8/2008 10:43:

When the Client Deployment page opens, you will see the client deployment folder views tree structure with the following predefined views:

- Notification batches.** Displays all the client deployment notifications batches sent from the client deployment center for a specific set of clients in your database.
- Notifications.** Displays all client notifications sent from the deployment center for all clients in your database.

- **Uncompleted notifications.** Displays all client notifications in your database for which the client installation has not been downloaded to a specific client.



If an end user downloads an installation package more than once for the same notification, and at least one download is successful, the notification will be considered completed and will not show up in Data Views, Client Deployment as an uncompleted notification. Additionally, if the last download attempt failed, the Last status details column will show the error, but the notification will be considered completed, and the Date Downloaded column will show the time of the last successful download.

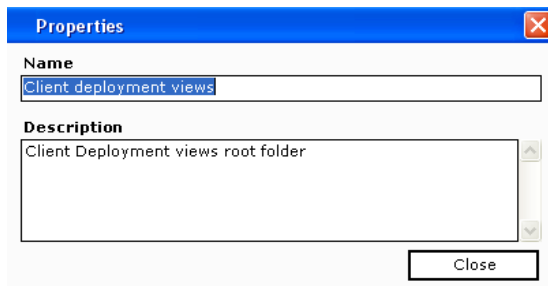
The following topics are included in this section:

- [“View folder properties and row counts” on page 493](#)
- [“Delete notification information” on page 494](#)
- [“View notification properties” on page 494](#)
- [“View notification batch information” on page 495](#)

View folder properties and row counts

You can view Client deployment folder properties and notification row count information from the left pane of the Client Deployment window.

To view Client deployment folder properties, click  **Properties** on the button bar or right-click the folder and choose **Properties** on the shortcut menu.



To view notification row count information, right-click on a notification and choose **Row Count** from the shortcut menu.



Delete notification information

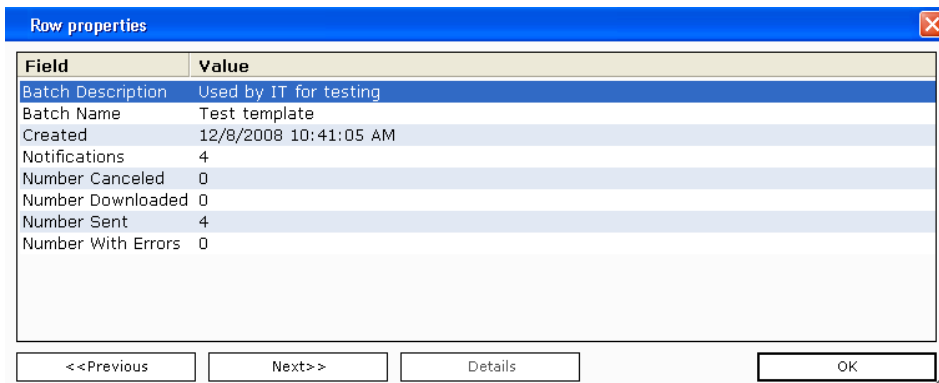
To delete Client deployment notification information:

- 1 Select a Client deployment view from the left pane to view the information in the right pane.
- 2 Right-click on a row from the right pane and choose **Delete** from the shortcut menu.

View notification properties

To view notification properties:

- 1 Select a Client deployment view from the left pane to view the information in the right pane.
- 2 Right-click a row from the right pane and choose **Properties** from the shortcut menu.



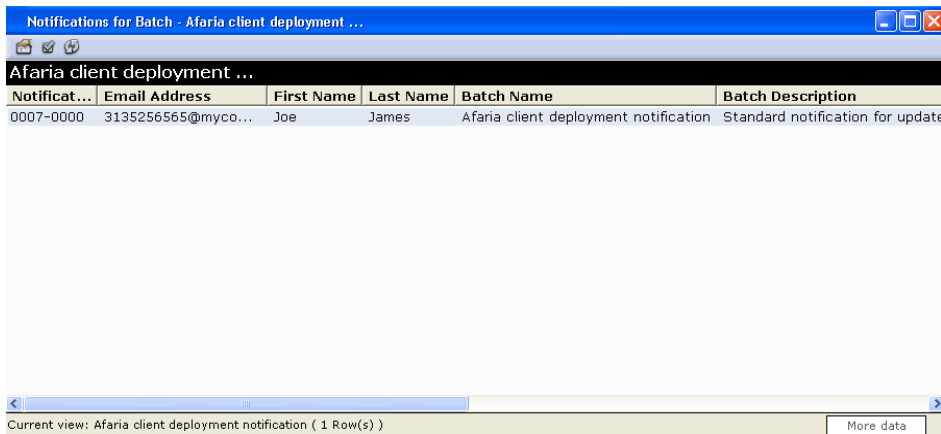
- 3 Click **Previous** or **Next** to view properties for other records.
If Notes have been entered about a specific field, click **Details** to view the information in the Item details dialog box.
- 4 Click **OK** to return to the Row properties dialog box.
- 5 Click **OK** again to return to Data views, Client Deployment.

View notification batch information

Notification batch information contains a record of all Client deployment notification messages sent to a Client or group of Clients in your database.

To view notification batch information:

- 1 Select a Client deployment view from the left pane to view the information in the right pane.
- 2 Right-click a row from the right pane and choose **Notification for Batch** from the shortcut menu.



The screenshot shows a window titled "Notifications for Batch - Afaria client deployment ...". The window contains a table with the following data:

Notificat...	Email Address	First Name	Last Name	Batch Name	Batch Description
0007-0000	3135256565@myco...	Joe	James	Afaria client deployment notification	Standard notification for update

At the bottom of the window, there is a status bar that reads "Current view: Afaria client deployment notification (1 Row(s))" and a button labeled "More data".

- 3 Click **More data** at the lower right corner of the window, if necessary, to display additional rows of information.



Index

A

Access points

- adding [86](#)
- copying [86](#)
- deleting [86](#)
- editing [86](#)
- properties [108](#)

Access policies

- roles, creating custom [45](#)
- users, adding and removing [42, 43](#)

Active sessions [69](#)

Address book

- adding entries [86](#)
- copying entries [86](#)
- CSV format [90](#)
- deleting entries [86](#)
- editing entries [86](#)
- importing addresses [89](#)
- maintaining distribution lists [88](#)
- maintaining entries [87](#)
- properties [87](#)

Administration

- Channels and channel sets [290](#)
- Monitors [316](#)
- Policies and Profiles [222](#)
- Replication, of channels [345](#)

Administrator, about [16](#)

alerts

- acknowledgement [76](#)
- alert definitions [193](#)
- assigned events [198, 203](#)
- closed [76](#)
- contact list [195](#)
- custom events [194](#)
- defined [193](#)
- defined contacts [194](#)

- details [73](#)

- Logs view [439](#)

- mail server [196](#)

- pending [77](#)

- properties [198](#)

- raised [72](#)

- repeat responses [201](#)

- response options [196, 200](#)

- SNMP [196](#)

- threshold [199](#)

- user-defined events [194](#)

Assignments

- groups to work profiles [231](#)

- LDAP [155](#)

- NT [155](#)

- replication sets to Servers [352](#)

- timeout [152](#)

Authentication

- channel security property [297](#)

- LDAP [155](#)

- NT [154](#)

- Server security [152](#)

- timeout [152](#)

B

Backup Manager

- alert thresholds [170](#)

- storage options [170](#)

Backup view

- Client representation [479](#)

- data

 - cleanup [481](#)

 - restore [480, 481](#)

- hardware representation [478](#)

- overview [477](#)

bandwidth throttling 115

BlackBerry Client

data lock/unlock 421

data wipe 421

device control options 421

inventory schema 365

C

cache

See compression cache

See differencing cache

Challenge code security response 425

Channel administration

about channel sets, components of 292

about channels, components of 292

auto actions 295

automatic subscriptions 294

channel parameter files (.XEC) 301

Channel Viewer options 297

channels in set, list and order of 298

Client type filter 292, 304

Clients running channels 292–293

create and manage channel set 306

create channel 304

general properties 294

icons defined 290

import/export channels 311, 312

outbound notification to run channel 314

publishing channels 307

security properties 296

set of channels 306

work profiles, associated list 300

work profiles, relationship to 290

Channel set

see Channel administration

Channel Viewer

running channels on Windows Clients 292

security attributes in channels 297

Channels

allowed list of, in work profile 240

properties, Package tracking view 468

see also, Channel administration

see also, Replication

status, Package tracking view 470

class 363

cleanup

Backup view data 481

failed sessions 133

logs 138

Client

Active sessions 69

Client actions in work profiles 223, 233

creation 15

data, restore 480, 481

dynamic groups 285, 286

groups

dynamic

Clients view 438

Inventory view 461

LDAP

Clients view 436

Inventory view 459

NT

Clients view 434

Inventory view 457

identifier 413, 479

identifier (GUID) 48

media 171

reassignments 48

representation, Backup view 479

running channels on 292–293

static groups 285, 287

tenants, association with

types

in work profiles 223

inventory schemas 364

Server configuration 189

Client deployment 85

access points 108

address book 85

CSV format 90

distribution lists 88

import addresses 89

notification messages 85

notification templates 91

prerequisites for notifications 101

self-service portal 85, 108

send notifications 101

toolbar 86

viewing information 492

Client groups

- configuring schedule for refresh [186](#)
- creating [285](#)
- dynamic [285](#)
- outbound notification addresses [360](#)
- outbound notifications [361](#)
- static [285](#)
- Client types**
 - filter in channels [292, 304](#)
 - filter in work profiles [229](#)
 - properties [192](#)
 - Windows Client parameters [190](#)
 - Windows Mobile Professional parameters [191](#)
- Clients view**
 - columns [390](#)
 - criteria, column [392](#)
 - data, delete [412](#)
 - data, remote wipe [422](#)
 - folder [432](#)
 - group
 - dynamic Client [438](#)
 - LDAP [436](#)
 - NT [434](#)
 - groups [434](#)
 - mini views [401](#)
 - overview [395](#)
 - properties
 - folder/view [433, 493](#)
 - row [409](#)
 - reassign a Client [413](#)
 - SQL
 - view [438](#)
 - view [432](#)
- CMX channel file** [311, 313](#)
- columns, view**
 - Clients view [390](#)
- compression cache**
 - configuring [117](#)
 - configuring schedule for refresh [186](#)
- configuration**
 - Backup Manager [170](#)
 - Document Manager [171](#)
 - Exchange ActiveSync policy [172](#)
 - file data [465](#)
 - Manager for SMS [179](#)
 - Relay server [163](#)
 - SMTP [158](#)
- contacts**

- alerts [194, 195](#)
 - defined alert [194](#)
 - properties [132](#)
- Create Client installation wizard**
 - overview [49](#)
 - seeding data [49](#)
- criteria**
 - column
 - Clients view [392](#)
- Crystal Reports, creating custom reports** [81](#)

D

- data**
 - cleanup, Backup view [481](#)
 - Client, delete [412](#)
 - Client, remote wipe [422](#)
 - configuration file [465](#)
 - directory scan [466](#)
 - hardware inventory [463](#)
 - restore, Client [480, 481](#)
 - seeding, Create Client installation wizard [49](#)
 - software inventory [464](#)
- Data Protection Manager**
 - recover password [425](#)
- Data views**
 - Backup view
 - Client representation [479](#)
 - data
 - cleanup [481](#)
 - restore [480, 481](#)
 - hardware representation [478](#)
 - overview [477](#)
 - BlackBerry device controls [421](#)
 - Client deployment [492, 493](#)
 - delete notification data [494](#)
 - folder properties [493](#)
 - predefined notification views [492](#)
 - view notification batch info [495](#)
 - Client revocation and approval [399](#)
 - Clients view
 - BlackBerry device controls [421](#)
 - Client data, delete [412](#)
 - Client data, remote wipe [422](#)
 - custom Clients view

- custom view [390](#)
- folder [432](#)
- groups [434](#)
- mini views [401](#)
- outbound notifications [417](#)
- overview [395](#)
- reassign a Client [413](#)
- recover password [425](#)
- SQL view [438](#)
- view [432](#)
- Inventory view
 - changes, acknowledge [462](#)
 - Client type inventory data [462](#)
 - folder [455](#)
 - groups [457](#)
 - monitor changes [453](#)
 - overview [452](#)
 - specific Client inventory data [463](#)
 - view [455](#)
- License compliance view
 - folder [484](#)
 - overview [482](#)
 - predefined views [483](#)
 - view [485](#)
- Logs view
 - Alerts [439](#)
 - Client deployment [443](#)
 - Client triggered actions [442](#)
 - export view [448](#)
 - File Transfers [440](#)
 - folder [445](#)
 - Handheld Security [443](#)
 - Messages [440](#)
 - overview [439](#)
 - Replication [441](#)
 - Sessions [442](#)
 - view [445](#)
 - Windows Security [444](#)
- outbound notifications [417](#)
- overview [363](#)
- Package tracking view
 - overview [467](#)
 - properties
 - channels [468](#)
 - status [471](#)
 - status, channel [470](#)
- Database
 - access [389](#)

- overview [363](#)
- Denied access state, Data Protection Manager
- device monitor. See Monitors
- Device provisioning
 - through OMA CP [94](#)
- differencing cache
 - configuring [128](#)
 - configuring schedule for refresh [186](#)
- Distribution lists
 - CSV format [90](#)
 - importing addresses [89](#)
 - maintaining [88](#)
 - properties [88](#)
 - sending access points [109](#)
 - sending notifications [101](#)
- Document Manager
 - Client media [171](#)
 - dependent files [171](#)
 - options [171](#)
- dynamic groups [285](#), [286](#)

E

- Email notifications
 - See Notifications
- Email-based SMS [158](#)
- Encryption
 - channel security property [297](#)
- event details, session [449](#)
- event monitor. See Monitors
- Events
 - raised events [74](#)
- events
 - assigned [198](#)
 - custom [194](#)
 - user-defined [194](#)
- Exchange ActiveSync policy
 - options [172](#)
- export, log view [448](#)

F

failed sessions

cleanup [133](#)

file transfers [440](#)

File type

CMX, channel import/export [311](#), [313](#)

PMX, work profile import/export [226](#), [227](#)

XEC, channel parameters [301](#), [303](#)

Free-form templates

properties [99](#)

sending [101](#)

G

Group profiles

about [223](#)

overview with diagram [223](#)

groups

dynamic [285](#), [286](#)

static [285](#), [287](#)

H

Home

Active sessions [69](#)

Alerts

acknowledgement [76](#)

closed [76](#)

details [73](#)

pending [77](#)

raised [72](#)

raised events [74](#)

Reports

See Reports

Server status

compression [67](#)

differencing [67](#)

sessions [67](#)

HTML

channel parameter files (.XEC) [301](#), [302](#)

I

Identifier for Clients [413](#), [479](#)

Identifier for Clients (GUID) [48](#)

Import/export

channels [311](#), [312](#)

work profiles [226](#), [227](#)

Importing addresses [89](#)

installation, Java Client [57](#)

inventory

changes, acknowledge [462](#)

data

Client specific [463](#)

Client type [462](#)

directory scan data [466](#)

hardware data [463](#)

monitor changes [453](#)

schemas

BlackBerry Client [365](#)

Palm Client [367](#)

Symbian Client [372](#)

Windows Client [373](#)

Windows Mobile Professional Client [368](#)

Windows Mobile Standard Client [370](#)

software data [464](#)

Inventory view

changes, acknowledge [462](#)

Client type inventory data [462](#)

configuration file data [465](#)

directory scan data [466](#)

folder [455](#)

group

dynamic Client [461](#)

LDAP [459](#)

NT [457](#)

groups [457](#)

hardware data [463](#)

monitor changes [453](#)

overview [452](#)

software data [464](#)

specific Client inventory data [463](#)

view [455](#)

J

Java Client, Afaria Client installation [57](#)

L

LDAP

- assignments [155](#)
- authentication [155](#)
- group, Clients view [436](#)
- group, Inventory view [459](#)
- security [152](#), [155](#)
- SSL [156](#)

License compliance view

- folder [484](#)
- overview [482](#)
- predefined views [483](#)
- properties, folder/view [485](#)
- view [485](#)

License compliance, schema [388](#)

License Manager

- configuring [206](#)
- schedule for compliance refresh [186](#)

licensing [134](#)

logging services

- alert logging [136](#)
- Client action logging services [136](#)
- messages [135](#)
- OMA DM Clients [442](#)
- policy [135](#)
- relay server outbound enabler events [163](#), [165](#)
- replication [135](#)
- session event details [135](#)
- session events [135](#)

logs

- cleanup configuration [138](#)
- policy configuration [135](#)
- schedule for cleanup [186](#)

Logs view

- Alerts [439](#)
- Client deployment [443](#)
- Client triggered actions [442](#)
- export, view [448](#)
- File Transfers [440](#)

folder [445](#)

Handheld Security [443](#)

Messages [440](#)

overview [439](#)

properties

- folder/view [446](#)

- row [449](#)

Replication [441](#)

session event details [449](#)

Sessions [442](#)

view [445](#)

Windows Security [444](#)

M

Manager for SMS

- configuration [179](#)
- schedule for refresh [186](#)

Message templates [92](#)

- properties [92](#)

- sending [101](#)

messages [440](#)

Monitor-action pairs [223](#), [233](#)

Monitors

- about [317](#)
- administration [316](#)
- common settings [324](#)
- connection monitor settings [325](#)
- creating [321](#)
- customized [336](#)
- deploying to Clients [319](#)
- editing [322](#)
- file/directory monitor settings [327](#)
- hours of operation [323](#)
 - about [323](#)
 - setting [323](#)
- list of types [317](#)
- monitor-action pairs [223](#), [233](#)
- schedule monitor settings [337](#)
- settings
 - connection [325](#)
 - file/directory [327](#)
 - memory [329](#)
 - power [331](#)
 - process [332](#)

- registry [335](#)
- schedule [337](#)
- window [344](#)

substitution variables [319](#)
support by Client type [319](#)
types [317](#)

Multitenancy

- add, delete, disable tenants [25](#)
- adding Afaria Clients [26, 27](#)
- assets, copying between tenants [31](#)
- assets, sharing between tenants [30](#)
- connecting clients [27, 28](#)
- creating Afaria Client packages [27](#)
- creating OMA DM Clients [27](#)
- defined [23](#)
- general workflow [25](#)
- introduction [23](#)
- reports, see Reports
- setting tenant context on pages [29](#)
- tenant list for user roles [25](#)
- the predefined system tenant [26](#)
- upgrading Clients [34](#)
- user role tenant list [45](#)

N

Notification templates [91](#)

- adding [86](#)
- copying [86](#)
- deleting [86](#)
- editing [86](#)
- Free-form [99](#)
- Message templates [92](#)
- OMA CP [93](#)

Notifications

- correcting invalid addresses [106](#)
- prerequisites [101](#)
- sending to addresses [101](#)
- sending to distribution lists [101](#)
- using a free-form template [103](#)
- using a message template [103](#)
- using an OMA CP template [103](#)
- validating addresses [106](#)

NT

- authentication [154](#)

- domains [153](#)
- group
 - Clients view [434](#)
 - Inventory view [457](#)
- security [152, 154](#)

O

OMA CP templates [93](#)

- basic properties [96](#)
- device differences [95](#)
- GPRS properties [96, 108](#)
- GSM/CSD properties [97, 109](#)
- homepage URL properties [97](#)
- how provisioning works [94](#)
- network PIN properties [98](#)
- sending [101](#)
- user PIN properties [98](#)
- validation [95](#)

OMA DM

- configure server [139](#)

OTA [15](#)

- configure download interface [142](#)
- definition [142](#)
- logging [143](#)

- See Message templates

- Web services interface [143](#)

OTA deployment center [139, 142](#)

OTA publisher

- launching from the Create Client wizard [52](#)

Outbound enabler service [163](#)

Outbound notification

- as public Web service [415](#)

- to run channel [361, 417](#)

Outbound notification to run channel

- as public Web service [314, 423](#)

- from channel view [314](#)

Outbound notifications

- about [226, 248, 289, 415](#)

Over the Air. See OTA

P

Package tracking view

overview [467](#)

properties

channels [468](#)

status [471](#)

status, channel [470](#)

Palm Client

inventory schema [367](#)

Password, recover [425](#)

Patch Manager

configuring [185](#)

configuring schedule for synchronization [186](#)

list of patches [212](#)

pending alerts [77](#)

Permanent Client identifier [413](#), [479](#)

Permanent Client identifier (GUID) [48](#)

Policies

in work profile [243](#)

Policies and Profiles

Administration [222](#)

see Group profiles

port

Server [131](#)

Profiles

see Group profiles

see Policies and Profiles

Properties

Relay server [163](#)

properties

Backup Manager [170](#)

bandwidth throttling [115](#)

cleanup [133](#)

compression [117](#)

contacts [132](#)

differencing [128](#)

Document Manager [171](#)

Exchange ActiveSync policy [172](#)

licensing [134](#)

log cleanup [138](#)

logging policy [135](#)

Manager for SMS [179](#)

OMA DM Server [139](#)

OTA deployment center [142](#)

security [152](#)

Server identification [131](#)

SMTP [158](#)

user-defined fields [159](#)

property [363](#)

Provisioning

through OMA CP [94](#)

Public Web service

outbound notification [415](#)

outbound notification to run channel [314](#), [423](#)

recover Data Protection Manager password [425](#)

R

raised

alerts [72](#)

events [74](#)

Reassign a Client [48](#), [413](#)

Recover password [425](#)

Relay server

configuration properties [163](#)

installing [163](#)

logging outbound enabler events [163](#), [165](#)

outbound enabler service [163](#)

Remote wipe command [422](#)

Replication

about [345](#)

advertising replication sets [348](#)

auto accept [355](#)

auto replicate [356](#)

channel refresh [349](#)

HTML parameter files [356](#)

logging services [135](#)

Logs view [441](#)

options properties [356](#)

overwrite option [356](#)

published status [356](#)

Schedule Editor [353](#), [354](#)

schedules [353](#)

Server farm environment [346](#)

Server to peer environment [347](#)

Servers

about [346](#)

properties [352](#)

registration [350](#)

- sets
 - about [346](#)
 - acceptance [355](#)
 - assignments [352](#)
 - automatic advertising of [349](#)
 - creation [348](#)
 - Server assignments [349](#)
- source and target [345](#)
- Reports**
 - about [79](#)
 - custom, creating with Crystal Reports [81](#)
 - graphical information and supporting details [80](#)
 - Report Information File (RIF) [82](#)
 - report results, about [79](#)
 - run a report [79](#)
 - XML schema definition (XSD) file [81](#)
- Response code for security challenge
- restoration, data [480](#), [481](#)

S

- scan, directory for inventory [466](#)
- Schedule Editor**
 - for Client tasks [353](#), [354](#)
 - for Server tasks [186](#), [187](#), [188](#)
- schedules**
 - daily [338](#)
 - monthly [338](#)
 - one time only [341](#)
 - replication [353](#)
 - weekly [338](#)
- schemas**
 - BlackBerry Client [365](#)
 - inventory [364](#)
 - License compliance [388](#)
 - overview [363](#)
 - Palm Client [367](#)
 - Server [385](#)
 - Symbian Client [372](#)
 - Windows Client [373](#)
 - Windows Mobile Professional Client [368](#)
 - Windows Mobile Standard Client [370](#)
- Security**
 - channel encryption [297](#)
- security**

- authentication [152](#)
- automatically approve Clients [156](#)
- Client approval [153](#)
- LDAP [152](#), [155](#)
- NT [152](#), [154](#)
- Security Manager**
 - See Data Protection Manager
- Self-service portal**
 - adding entries [86](#)
 - copying entries [86](#)
 - deleting entries [86](#)
 - device types [111](#)
 - editing entries [86](#)
 - platforms [110](#)
- Sending notifications** [101](#)
- Serialized and un-serialized devices** [48](#), [413](#), [479](#)
- Server**
 - about [15](#)
 - contacts [132](#)
 - identification [131](#)
 - licensing [134](#)
 - properties [113](#)
 - schedules [186](#)
 - schema [385](#)
- Server configuration**
 - alert definitions [193](#)
 - Client types [189](#)
 - license compliance [206](#)
 - properties [113](#), [139](#), [142](#)
 - Backup Manager [170](#)
 - bandwidth throttling [115](#)
 - compression [117](#)
 - contacts [132](#)
 - differencing [128](#)
 - Document Manager [171](#)
 - Exchange ActiveSync policy [172](#)
 - failed session cleanup [133](#)
 - license [134](#)
 - log cleanup [138](#)
 - logging policy [135](#)
 - Manager for SMS [179](#)
 - OTA deployment center [139](#), [142](#)
 - Relay server [163](#)
 - security [152](#)
 - Server identification [131](#)
 - SMTP [158](#)

- user-defined fields [159](#)
- Server schedules [186](#)
- Server farms
 - about [17](#)
 - see also, Replication
- Server list
 - Access policies [38](#)
- Server status
 - compression [67](#)
 - differencing [67](#)
 - sessions [67](#)
- Servers
 - adding and removing [40, 41](#)
 - see also, Replication
 - server list [38](#)
 - status [67](#)
- session, event details [449](#)
- sessions [442](#)
 - active [69](#)
 - cleanup [133](#)
- Short Messaging Service
 - definition [144](#)
- SMS
 - channel import [181](#)
 - channel settings [182](#)
 - check file options [182](#)
 - collections [180](#)
 - package settings [183](#)
 - send file options [183](#)
 - servers [180](#)
- SMTP configuration [158](#)
- SMTP server [158](#)
- Software Catalog Editor [15](#)
- SQL
 - view, Clients view [438](#)
- SSL
 - LDAP [152, 156](#)
- static groups [285, 287](#)
- Symbian Client
 - inventory schema [372](#)

T

- Templates
 - See Notification templates
- Temporary recovery password [425](#)
- Tenant, see Multitenancy
- throttling [115](#)
- transfers, file [440](#)

U

- Unique Client identifier [413, 479](#)
- Unique Client identifier (GUID) [48](#)
- Un-serialized and serialized devices [48, 413, 479](#)
- updates, Clients [60](#)
- user-defined fields [159](#)
- Users
 - about user roles [44](#)
 - adding and removing [42](#)
 - adding tenants for [45](#)

V

- View
 - custom views [390](#)
- view
 - custom
 - Clients view [432](#)
 - Inventory view [455](#)
 - License compliance view [485](#)
 - Logs view [445](#)
 - log view, export [448](#)
 - SQL, Clients view [438](#)
- views, mini, Clients view [401](#)

W

- Web service
 - outbound notification [415](#)

outbound notification to run channel [314](#), [423](#)
recover Data Protection Manager password [425](#)

Windows Client

inventory schema [373](#)

Windows Mobile Professional Client

inventory schema [368](#)

Windows Mobile Standard Client

inventory schema [370](#)

Work profiles

allowed channels, about [224](#), [240](#)

assign groups to [223](#), [231](#)

channel, default [229](#)

Client action

about [233](#)

automated [223](#)

Criteria attribute [238](#)

execute program [236](#)

log event only [236](#)

Retries attribute [238](#)

run channel or set [236](#)

run script [237](#)

support by Client type [235](#)

Client type filter [229](#)

Client types in [223](#)

create, edit, copy, delete [225](#)

examples for implementation [244](#)

group All Clients [231](#)

import/export [226](#), [227](#)

monitor-action pairs [223](#), [233](#)

policies, about [243](#)

X

XEC channel parameter file [301](#), [303](#)