



PUBLIC
2019-01-16

SAP Afaria Overview

Content

- 1 Afaria Overview. 3**
- 1.1 About Afaria. 3
- 1.2 Afaria Access and Support. 4
- 1.3 Finding Information. 5

- 2 Data Protection and Privacy. 7**

- 3 Afaria Architecture. 9**

- 4 Afaria Components. 11**
- 4.1 The Afaria Server. 12
- 4.2 Afaria Administration Console. 12
- 4.3 The Enrollment Server. 12
- 4.4 The Package Server. 13
- 4.5 The Self-Service Portal. 13
- 4.6 The SMS Gateway. 13

- 5 Typical Deployment Scenario. 15**

- 6 Network Ports. 16**

- 7 Required Active Directory Account Permissions. 20**

- 8 Estimating Your Database Size Requirements. 21**

1 Afaria Overview

This section provides an overview of Afaria, its features, architecture, and components. It describes how Afaria interacts with other systems and devices on your network such as your Active Directory server, Exchange server, and firewall.

1.1 About Afaria

Afaria is a mobile device management (MDM) system that allows you to secure and manage your organization's mobile devices, mobile applications, and data. With Afaria, you can remotely connect to mobile devices enrolled with Afaria in order to configure the device and install required applications. Afaria is part of the Mobile Secure suite of products from SAP that includes Mobile Docs and Mobile Apps.

With Afaria, you can:

- Secure devices and device data. Afaria includes a number of features and technologies to secure enrolled devices. For example, Afaria leverages existing security infrastructures on your network such as Active Directory and LDAP to ensure only users known to your network can access your network. Afaria also uses certificates to secure connections between Afaria and the device. Finally, Afaria can leverage security features on the device, for example, to enforce a password or encrypt a device storing sensitive corporate data. You can also use Afaria to remotely lock lost or stolen devices and even "wipe" the device of corporate data.
- Configure devices to meet corporate standards. With Afaria, you can define and maintain device attributes and settings to ensure that your mobile devices are configured properly for your network. For example, Afaria can manage ActiveSync settings, including connection settings, and synchronization options. You can also use Afaria to remotely configure connection settings, such as details about the network service, server addresses, and login. Synchronization options for email, calendar and contact information can be configured centrally and enforced on client devices.
- Manage mobile applications. With Afaria, you can ensure that all devices have the latest versions of all necessary software. Afaria makes it easy to distribute, install, and maintain mobile applications, both in-house apps and publically available on an application store like Apple's App Store or Google Play. Afaria's ability to install applications, supply missing or corrupted files, and uninstall or roll back applications means that all your employees will have the correct versions, the latest updates, and the right settings at all times.
- Control corporate assets and report on mobile device usage. With Afaria, you can view device inventory including who is using the device, what software is installed, and what settings are configured.

Afaria can manage both corporate and employee-owned devices as part of a corporate Bring-Your-Own-Device (BYOD) program. Afaria supports Android, iOS, Windows, Windows CE, Windows Mobile, Windows Phone, and Windows with the MDM client (Windows DM) devices.

1.2 Afaria Access and Support

SAP provides industry-leading support and a variety of downloads to help you get the best out of your products and solutions.

The sections below provide more information about getting access to Afaria, Afaria support, and Afaria documentation.

Where to Get Afaria

Visit the [Afaria Software Download](#) page on the SAP Support portal to download Afaria.

You will require a Download Software authorization, which you can request from your company's SAP System Administrator.

Afaria Support

To get access to Afaria information and report incidents, go to the SAP [Support portal](#). Use these links for [Afaria Support Documentation](#) and [Afaria Release Notes](#).

Registering for Notifications

Manage notifications for SAP Notes and knowledge-based articles (KBAs) using the Expert Search feature of the Support Portal. For help on setting up notifications, refer to the [Working with the Expert Search](#) topic in the My SAP Notes & KBAs online help.

You can also check out this [blog](#) for more information.

Afaria Documentation

For module-wise documentation of Afaria, refer to the SAP Afaria 7 SP32 section of the SAP Help portal (https://help.sap.com/viewer/p/SAP_AFARIA).

Contact Us

To learn more about the SAP Support portal, check the help topics at <https://support.sap.com/support-programs-services/about/help-index.html>.

For any feedback or queries related to Afaria Technical Publications, contact us at pubs@sap.com.

1.3 Finding Information

Afaria documentation is organized into a number of self-contained modules for quick reference.

- *Afaria Overview* – This module describes Afaria, its features, architecture, and components. It describes how Afaria interacts with other systems and devices on your network such as your Active Directory server, Exchange server, and firewall.
- *Preparing to Install Afaria* – This module provides the tasks to prepare your environment for the installation of Afaria. It includes information on how to configure your database, Windows server, and Certificate Authority for Afaria operations. It also describes how to acquire and import Apple certificates required for iOS device management.
- *Installing Afaria* – This module provides the tasks to install Afaria components such as the Afaria Server, the Enrollment Server, the Package Server, and the Self-Service Portal.
- *Configuring Afaria* – This module provides the tasks to configure Afaria using the Afaria. It describes the settings on the Server configuration pages and includes tasks for configuring the Afaria Server and components, creating roles and tenants, and setting security settings.
- *Device Management* – This module provides the tasks for managing devices including creating groups, creating application and configuration policies, enrolling devices, and administering and monitoring devices.
- *Server Monitoring* – This module provides information about monitoring Afaria.

For information about...	See...
Installing Afaria components	<ol style="list-style-type: none">1. <i>Afaria Overview</i> for system requirements and descriptions of Afaria components.2. <i>Preparing to Install Afaria</i> for steps to create a database for Afaria and to configure your servers and network for Afaria operation.3. <i>Installing Afaria</i> for descriptions of the settings in the installation wizards.4. <i>Configuring Afaria</i> for the steps to configure Afaria components in the Afaria Administration console.
Upgrading Afaria	<ol style="list-style-type: none">1. <i>Upgrading Afaria</i> for upgrade information and steps including preparing your installation for upgrade.2. <i>Installing Afaria</i> for descriptions of the installation wizards.
Setting up access control	<ol style="list-style-type: none">1. <i>Installing Afaria</i> if you plan on installing Access Control Filter components. This is not required for Access Control Remote setup.2. <i>Configuring Afaria</i> for the steps to configure the Access Control Filter. This is not required for Access Control Remote setup.3. <i>Device Management</i> for the steps to create access control policies.
Installing Apple certificates for iOS	<ol style="list-style-type: none">1. <i>Preparing to Install Afaria</i> for the steps to generate or download Apple certificates.2. <i>Configuring Afaria</i> for the steps to install the APNs certificate.

For information about...	See...
Enrolling devices	<i>Device Management</i> for the steps to create groups, enrollment policies, and configuration policies.
Monitoring SAP Afaria	<i>Server Monitoring</i> for information about viewing log files and events.
Managing certificates	<ol style="list-style-type: none"> 1. <i>Preparing to Install Afaria</i> for the steps to configure your CA and installing a CA proxy. 2. <i>Configuring Afaria</i> for the steps to create CA profiles and associate them with the Enrollment and Package servers. 3. <i>Device Management</i> for the steps to create configuration policies that include certificate requests and to revoke and renew certificates on managed devices..

2 Data Protection and Privacy

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy regulation, it is necessary to consider compliance with industry-specific legislation in different countries.

Context

SAP provides specific features and functions to support compliance with regard to relevant legal requirements, including data protection. SAP does not give any advice on whether these features and functions are the best method to support company, industry, regional, or country-specific requirements. Furthermore, this information should not be taken as advice or a recommendation in regards to additional features that would be required in specific IT environments; decisions related to data protection must be made on a case-by-case basis, taking into consideration the given system landscape and the applicable legal requirements.

i Note

SAP does not provide legal advice in any form. SAP software supports data protection compliance by providing security features and specific data protection-relevant functions, such as simplified blocking and deletion of personal data. In many cases, compliance with applicable data protection and privacy laws will not be covered by a product feature. Definitions and other terms used in this document are not taken from a particular legal source.

Important Terms

Term	Definition
Consent	The action of the data subject confirming that the usage of his or her personal data shall be allowed for a given purpose. A consent functionality allows the storage of a consent record in relation to a specific purpose and shows if a data subject has granted, withdrawn, or denied consent.
Deletion	The irreversible destruction of personal data.
Personal data	Any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Term	Definition
Mobile service and set-up	Any information related to using the mobile service and setting up access, authentication, operations, security, and so forth. It may be related to a "data subject" but in the context of processing authentication, data, usage, and so forth.
Purpose	A legal, contractual, or in other form justified reason for the processing of personal data. The assumption is that any purpose has an end that is usually already defined when the purpose starts.

Support for Data Protection and Privacy Standards

SAP Afaria supports the following actions pertaining to data protection and privacy standards:

Erasure of personal data The delete device action removes all personal data for a given device.

Logging changes to personal data Some user/device data can be edited, but all changes are logged.

Report or display function to inform users about the personal data stored about them The SAP Afaria Self-Service Portal allows users to retrieve a copy of the information stored in the system about them and any devices associated with those users.

Logging read access to sensitive personal data SAP Afaria creates log entries for the following events:

- Each time a standard query or custom data view is run.
- Whenever the device inspector is opened for a given device.

Capture explicit user consent before collecting any personal data User consent is handled in the following ways:

- iOS – User consent is handled by the OS during the MDM enablement process.
- Android – User consent is handled by the OS during app installation.
- Windows Phone – Customers can include user consent text in SAP Afaria Self-Service Portal and Mobile Place EULA.
- Windows DM – Customers can include user consent text in SAP Afaria Self-Service Portal EULA.
- Windows Mobile – EULA during installation of the Windows Mobile client.
- Windows 32 – EULA during installation of the Windows client.

3 Afaria Architecture

Afaria is a distributed mobile device management system consisting of a number of separate software components. The main components are the Afaria Server, the Afaria Administration Console, the Enrollment Server, the Package Server and the Afaria database. See Afaria components for more information.

The Afaria solution is highly scalable and can support very large installations. You can install Afaria on a single server ("standalone") for small installations or distribute Afaria across a number of servers for larger installations. For large installations, you can install multiple Afaria Servers in a farm scenario. In this scenario, the first Afaria Server you install is the "master" server; additional Afaria Servers are referred to as farm servers. The master server can speak with multiple farm servers to handle load balancing and support hundreds of thousands of remote connections with managed devices. In this environment, Afaria can synchronize content across distributed servers, which may be located in different locations. Any server that the client communicates with has identical functionality.

In an Afaria Server Farm scenario, the source Server (or master) is the Server where all channels are created, edited and managed. These channels are replicated to the target Servers (or slaves) in the Server Farm. Afaria Clients can connect to any Server in the farm and run the assigned channels. This provides a type of load-balancing solution if you have many Clients scheduled to connect at one time. Groups of Clients can connect to any Server in the farm to run the necessary channels.

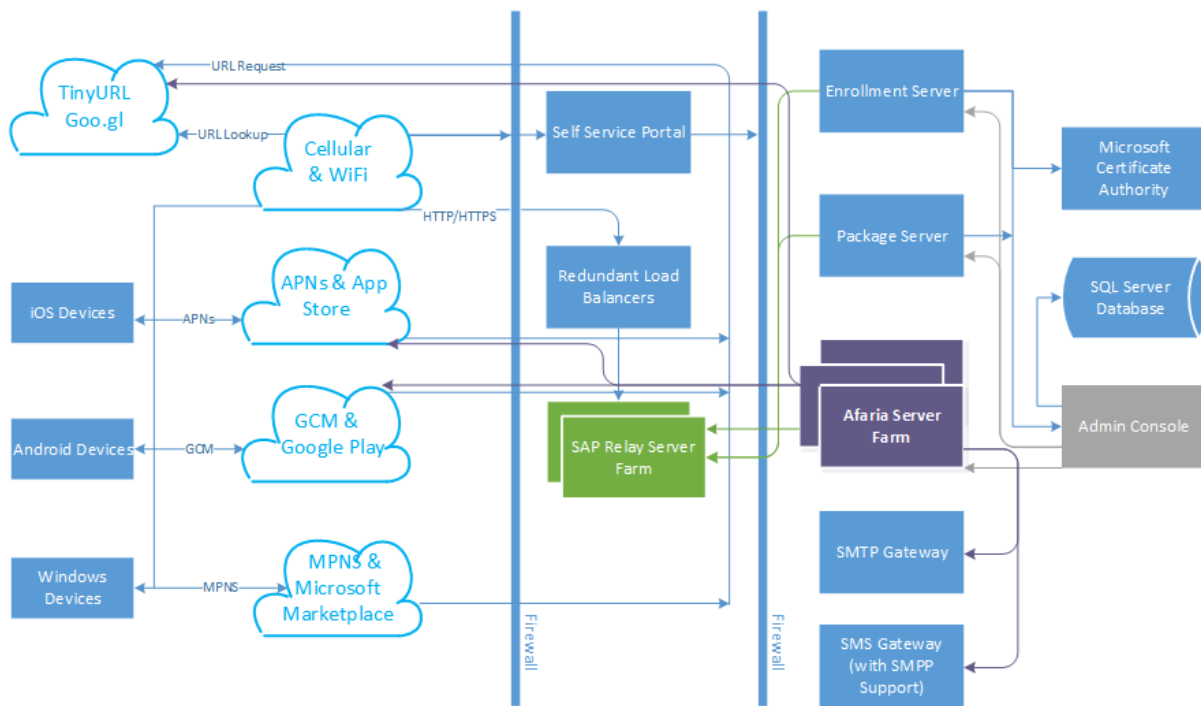
A Distributed Server environment is comprised of a group of Servers, operating independently and generally in different physical locations whose functionality is driven in whole or in part by a single Master server. Distributed Afaria Server farms support the local use of an independent Afaria database that contains information about logging, inventory, and alerts data for only the server they support. A dynamically elected machine in the Server farm runs the alerts rules engine and the alerts notification, as well as change detection for all Servers, but only for shared functionality.

In a Distributed Afaria Server scenario, the source Server (or master) is the Server where all management tasks are created, edited and managed. These policies are replicated to the target Servers; Clients can connect to any Server in the farm and run the assigned policies. This provides a type of load-balancing solution if you have many Clients located across heterogeneous geographies. Groups of Clients can connect to a local server, thus avoid communication and congestion delays inherent in a WAN environment.

Afaria supports either an Microsoft SQL Server or SAP SQL Anywhere database. Database server software is not shipped with Afaria. See Afaria Components for more information.

An Afaria Server Farm supports the shared use of a centralized Afaria database that contains information about logging, inventory, and alerts data across all Afaria Servers that are members of the farm. A dynamically elected machine in the Server farm runs the alerts rules engine and the alerts notification, as well as inventory change detection for all Servers.

The Relay Server is reverse proxy server and is included with Afaria to manage incoming connections from remote devices. Relay Server can also be configured in a farm scenario).



A Typical Afaria Installation – Internet, DMZ, and Enterprise Network

- Internet – devices and public entities.
 - Devices – user devices, such as smartphones and computers that Afaria manages. Devices either have an Afaria application installed or have a native capability that Afaria uses to interact with the hosting device. Devices connect to Afaria servers or their proxies using HTTP and SSL.
 - Public entities and services – entities that support device management and features, such as the Apple Push Notification Service (APNS) for managing iOS devices, or a commercial application market for Afaria application policies.
- DMZ – relay or proxy servers, such as a Microsoft Forefront Threat Management Gateway server or a SAP Sybase SQL Anywhere Relay Server to enforce firewall rules and receive device communication before relaying it to an Afaria server in the enterprise network. For Access Control for Email, an optional feature, the e-mail proxy server hosts the access control filter to allow or block incoming requests based on access control policy information from Afaria. Using relay servers in the DMZ to relay communication is optional, but recommended to increase enterprise network security.
- Enterprise network – the component servers and the email network require connectivity to the Afaria server, and sometimes the database. When relay servers are configured for the components, Afaria servers receive incoming communication from the relay servers, rather than directly from the Internet.
 - You can consolidate some or all the server components on to fewer servers, or on to a single server.
 - If devices are resident within the enterprise network, you can configure them to make direct connections to Afaria servers.

4 Afaria Components

The main Afaria components are:

- **Afaria Server:** Communicates with devices under MDM control applying configuration policies and collecting inventory data.
- **Afaria Administration console:** A web-based user interface for Afaria for configuring Afaria, managing devices, and reporting on TEM and inventory.
- **Enrollment Server:** Handles the enrollment of devices with Afaria and also delivers management payloads for iOS devices. The enrollment server should be installed on the same server as the Afaria Server.
- **Package Server:** Serves Afaria application packages to devices and also handles certificates and device provisioning data to calling third-party applications. The portal package server does not serve commercial applications to devices.
- **Self-Service Portal:** Lets end-users enroll their device in Afaria management, and lets users view their device information and issue commands, such as to reset a password. The portal is optional for enrollment and allows users to install application policies with support from the package server.
The Self-Service Portal is for deployment inside the enterprise firewall with an Internet-facing Microsoft Forefront Threat Management Gateway instance in the DMZ configured to accept device connections and pass traffic to the internal portal.

Afaria also ships with a number of optional components and software packages:

- **SMS Gateway:** Handles SMS messages such as outbound notifications and remote wipe commands. The SMS Gateway uses the Cygwin product libraries and tools from Cygnus Solutions as well as other open source tools. The SMS Gateway is not required for Afaria operation.
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 servers notification messages, and any other Afaria communication that is addressed for SMS routing.
- **Relay server:** A proxy for HTTP and HTTPS connections from the Internet to a component server, such as the Afaria server or the enrollment server. The relay server is optional, but recommended for increased enterprise network security.
- **Access Control for Email:** Access Control components allow you restrict access to corporate email
- **Network Access Control:** Network Access Control (NAC) allows you to restrict access to your network.

Afaria also connects with the following components on your network:

- **Afaria database** – SAP SQL Anywhere or Microsoft SQL database that stores procedures; configuration properties; device, group, and policy data; and all message and activity logging. For Afaria server components, access to the database is either direct to the database or indirect through the Afaria server.
- **Certificate Authority** – certificate authority definitions are assigned to the enrollment and package servers to support enrollment of devices or to facilitate certificate provisioning for application onboarding.
- **E-mail Server** – for Access Control for corporate e-mail, an optional feature, the server hosts the access control PowerShell service, which polls the Afaria server for current access control policies, and delivers that information to the e-mail proxy in the DMZ. For Access Control for hosted e-mail, e-mail hosting is on the Internet and does not include an e-mail server in the enterprise.

4.1 The Afaria Server

The Afaria Server control the communications between the mobile devices and determine the actions taken during a communications session.

It can operate as a single, standalone server, or as multiple servers in a server farm. The server communicates with the Afaria database and additional components or devices as necessary.

- Standalone Afaria server – a single Afaria server operating as the only server in an installation. The server has a one-to-one relationship with the database.
- Afaria Server farm – multiple Afaria Servers operating together in an installation. The servers have a many-to-one relationship with the database. A server farm includes one master Afaria Server and one or more farm servers.

Redundancy is provided by adding additional slave servers to an environment. The Afaria Server design is as such that any single Afaria Server can go down without effecting any other Afaria server in the environment. When a server ceases to function, the Relay Server stops directing traffic to that server.

4.2 Afaria Administration Console

The Afaria Administration console is a web-based utility for managing and configuring SAP Afaria.

The Afaria Administration console has very granular role-based administration that allows easy setup of user rights whether they are an administrator or help desk, or any number of customizable roles.

The web console has many features including:

- Customizable reporting
- Intuitive streamlined workflow
- Granular customizable role/rights based administration
- Easy policy and group assignments
- Comprehensive API for enterprise integration

4.3 The Enrollment Server

The Enrollment Server is required in order to provision devices. It also serves a purpose in identifying the software packages to be pushed to the device.

Afaria Enrollment Server resource recommendations are based on concurrent client sessions and session duration. The following factors can affect session duration:

- Device response time
- Number of device configuration policies
- Number of settings within device configuration policies

- Connection speed
- IIS server request processing capacity
- Recommendations are for one server for 200-500 concurrent sessions with iOS devices

The Enrollment Server requires that the Afaria Master Server remain available in order to function, thus providing a single point of failure for Package Server functionality.

4.4 The Package Server

The Package Server hosts custom developed applications as well as definitions for platform application stores. This component is configured through the Afaria Administration console.

The Package server resource recommendations are based on concurrent client sessions and session duration. The following factors can affect session duration:

- Device response time
- Number of device package assignments
- Size of application packages
- Connection speed
- IIS server request processing capacity

Each Package Server acts independently. Providing redundancy is as simple as installing the Package Server on another IIS Server. Configuring the Package Server to use the Relay Server for indirect access allows connectivity to be controlled via the Relay Server to any running Package Server. The Package Server requires that the Afaria Master Server remain available in order to function, thus providing a single point of failure for Package Server Functionality.

4.5 The Self-Service Portal

Use the Self-Service Portal to enroll Android, iOS, Windows DM (Windows 8.1), Windows Phone, or Windows Mobile devices in Afaria management, to view device information, and to issue commands such as to remote lock or remote wipe a device.

For more information on installing and upgrading Self-Service Portal and configuring Self-Service Portal, refer the *Installing Afaria* and *Configuring Afaria* documentation modules respectively on SAP Help Portal.

4.6 The SMS Gateway

The SMS Gateway is an optional third-party software component available for use with Afaria. The gateway handles SMS messages such as outbound notifications and remote wipe commands. The SMS Gateway uses the Cygwin product libraries and tools from Cygnus Solutions as well as other open source tools. The SMS Gateway is not required for Afaria operation.

SMS Gateway requires a certificate known to both Windows and Linux:

- Windows: The certificate and its associated key must be a visible Windows Trusted Root Certificate Authority. The Windows Trusted Root is accessible only to the Afaria Server.
- Linux: 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.

See SMS install and configuration for details.

5 Typical Deployment Scenario

A typical scenario would have the Afaria Server, Administrator Console, and database on separate servers. However, how you deploy Afaria will depend on the your needs and environment.

SAP will consult with you to develop a deployment plan that is appropriate for the specific environment. Some factors influencing the and will depend on various factors, such as the total number of clients, the total number of anticipated concurrent clients, and whether you would like to plan for peak or average concurrency.

6 Network Ports

This topic provides the ports required for various network connections.

Device to Perimeter

Source	Destination	Protocol	Port	Notes
Device	Relay Server(s)	http/https	80/443	Can be load balanced to multiple relay servers. SSL is required for iOS
Device	Self Service Portal	http/https	80/443	SSL is optional
Device	iTunes Store	http	80	iOS only, for download of Afaria app (or other apps if desired)
Device	Google Play Store	http	80	Android only

Perimeter to Internal

Source	Destination	Protocol	Port	Notes
Self Service Portal	Afaria API Service/ Administrator	TCP	7982, 8085	
Self Service Portal	Afaria Server(s)	TCP (DCOM)	135, 5000-5100	Required for device actions which require immediate notifications (wipe, lock, unlock)

Internal to Perimeter

Source	Destination	Protocol	Port	Notes
Afaria Server(s)	Relay Server(s)	http/https	80/443	SSL optional
Enrollment Server	Relay Server(s)	http/https	80/443	SSL optional

Source	Destination	Protocol	Port	Notes
Package Server	Relay Server(s)	http/https	80/443	iOS / Android only SSL optional
Certificate Authority	Relay Server(s)	http/https	80/443	iOS only SSL optional

Internal to Internal

Source	Destination	Protocol	Port	Notes
Enrollment Server	Afaria Server(s)	tcp (DCOM)	135, 5000-5100	
Enrollment Server	Afaria Server(s)	tcp	8085-8087	
Package Server	Afaria Server(s)	tcp (DCOM)	135, 5000-5100	
Package Server	Afaria Server(s)	tcp	8085-8087	
Package Server	Certificate Authority	http/https	80/443	

Internal to Database

Source	Destination	Protocol	Port	Notes
Afaria Server(s)	DB Server	tcp	1433 (MSSQL) 2638 (SQL Anywhere)	
Afaria Admin/ API Service	DB Server	tcp	1433 (MSSQL) 2638 (SQL Anywhere)	
Enrollment Server	DB Server	tcp	1433 (MSSQL) 2638 (SQL Anywhere)	
Package Server	DB Server	tcp	1433 (MSSQL) 2638 (SQL Anywhere)	iOS/Android only
Certificate Authority	DB Server	tcp	1433 (MSSQL) 2638 (SQL Anywhere)	iOS only; Only required if using SCEP plugin

Admin to Internal

Source	Destination	Protocol	Port	Notes
Browser	Afaria Administrator/ API Service	http/https	80/443	Admin browser for managing servers SSL optional
Afaria Administrator/ API Service	Afaria Server(s)	TCP	8085-8087	

Source	Destination	Protocol	Port	Notes
Afaria Administrator/ API Service	Afaria Server(s)	TCP (DCOM)	135, 5000-5100	

Internal to External

Source	Destination	Protocol	Port	Notes
Afaria Server(s)	iTunes Store	http	80	iOS only Used for displaying app information / icons in portal
Afaria Server(s)	APNs	tcp	2195/ 2196	iOS only Data/ Feedback ports
Afaria Server(s)	Google Play Store	http	80	Android only Used for displaying app information / icons in portal
Afaria Server(s)	C2DM (android.googleapis.com)	https	443	Android only
Afaria Server(s)	TinyUrl URI Service (tinyurl.com)	http	80	Required for enrollment code support (either tinyurl or goo.gl)
Afaria Server(s)	Goo.gl URL Service (goo.gl)	http	80	Required for enrollment code support (either tinyurl or goo.gl)
Afaria Server(s)	SMTP Server	smtp	25	Used for sending email messages to users/ administrative alerts
Afaria Server(s)	SMPP/SMS Gateway	smpp	13000	Used for sending SMS messages to devices. Port varies.

Device Network Requirements

Source	Destination	Port
Apple/iOS	gateway.push.apple.com, feedback.push.apple.com	5223

Source	Destination	Port
Apple/iOS	gateway.sandbox.apple.com (for developers)	5223
Apple/iOS	IP Range: 17.0.0.0/8	5223
Google/GCM/C2DM	android.googleapis.com	5228 (and sometimes 5229, 5230)
Google/GCM/C2DM	74.125.0.0/16	5228 (and sometimes 5229, 5230)
Google/GCM/C2DM	IP Ranges provided as part of Google's ASN of 15169	5228 (and sometimes 5229, 5230)

7 Required Active Directory Account Permissions

If you intend to use Active Directory authentication for your SQL Server database, you'll need to grant appropriate permissions to the user account you specify for connecting to Active Directory.

To manage and monitor changes in Active Directory, explicitly grant the user account the Replicating Directory Changes permission. The account does not need to belong to the Domain Administrator group; Any user explicitly granted the Replicating Directory Changes permission will have the necessary privileges.

This account must also have rights to read the token group attribute of user objects in order for user group policy assignments to work. This permission is usually granted by default. Ensure that it hasn't been manually revoked.

To allow the account to discover objects in Active Directory using the Active Directory management agent (ADMA), ensure the permission is granted for every domain that the management agent accesses.

To create, modify, and delete objects within Active Directory using a non-administrative account, grant additional permissions as appropriate.

For example, for Microsoft Metadirectory Services (MMS) to create new user objects in an Organizational Unit (OU) or container, the account that is used must be explicitly granted the Create All Child Objects permission, as the Replicating Directory Changes permission is not sufficient to allow the creation of objects.

8 Estimating Your Database Size Requirements

To understand your weekly disk space requirements for operations with all logging enabled, estimate your database size. Plan disk availability based on requirements.

Procedure

1. Estimate values:
 - Number of sessions per day
 - Average session size
2. Apply the estimates to the daily formula for estimated growth per day:
 $(\# \text{ of sessions per day}) * (\text{average session size}) = \text{estimated growth per day}$
3. Apply the daily estimate to the weekly formula for estimated growth per week:
 $(\text{estimated growth per day}) * 7 = \text{estimated growth per week}$

❖ Example

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

$(1000 \text{ sessions per day}) * (60\text{KB average session size}) * 7 \text{ days} = 420\text{MB}$

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

Consider these items for calculating estimates:



- Add 1MB of data per week to the estimate for each device that reports inventory.
- Session channels with 100 events add an average of 40KB in database growth per session in additional log data.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
 - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
 - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

© 2019 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.