PUBLIC
2019-01-16

SAP Afaria 7 SP32 Release Notes

THE BEST RUN SAP

Content

1 About These Release Notes

These Release Notes are current as of SAP Afaria 7 SP32.

LEGAL Disclaimer

The information in this document is proprietary to SAP and may not be distributed without the permission of SAP. This document is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this document is not a commitment, promise or legal obligation to deliver any material, code or functionality. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This document is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP´s willful misconduct or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

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.

3 What's New in SAP Afaria

The new features, enhancements, and changes introduced in Afaria are:

SP32

Area	Feature	Documentation Location
System Requirements	SAP is discontinuing support for older operating system versions, database server versions, browser versions, and other third-party product versions	See SAP Note #2707564 for details.

SP31

Area	Feature	Documentation Location
iOS Support	Support for iOS 12.1 devices.	SAP Afaria System Requirements > Device Requirements > iOS Devices
APNS Support	Apple's APNs based on the HTTP/2 network protocol.	See next section, Setting up Apple APNs Certificates for Afaria 7 SP31 [page 26].

SP30

Area	Feature	Documentation Location
Google Cloud Messaging (GCM) and Firebase Cloud Messaging (FCM)	Google Cloud Messaging (GCM) and Firebase Cloud Messaging (FCM) are now interoperable. The October 2018 release of the Mobile Secure Android client uses Google's FCM libraries rather than the GCM libraries. Existing devices upgraded to the new client will still be able to receive outbound messages from Afaria Servers configured to use GCM.	Configuring SAP Afaria > Server Configuration for Installation and Management > Afaria Server for GCM > Configuring Firebase/Google Cloud Messaging

Area	Feature	Documentation Location
Android Support	Support for Android 9.0 devices.	SAP Afaria System Requirements > Device Requirements > Android Devices
Windows Server Support	Support for Windows Server 2016 (with one known issue, see Upgrading Afaria [page 33])	SAP Afaria System Requirements: • > SAP Afaria Server Requirements • > Certificate Authority Requirements • > SAP Afaria Administrator Requirements • > Network Access Control Requirements • > Self-Service Portal Requirements • > Package Server Requirements • > Enrollment Server Requirements

SP29

Area	Feature	Documentation Location
iOS Support	Support for iOS 12, iOS 11.4.x, 11.3.x, 11.2.x, and 11.1.x devices	SAP Afaria System Requirements > Device Requirements > iOS Devices
System Requirements	Support for the following versions of Microsoft SQL Server: • Microsoft SQL Server 2016 Enterprise edition • Microsoft SQL Server 2016 Standard edition	SAP Afaria System Requirements > Database Requirements

SP28

Area	Feature	Documentation Location
Afaria Self-Service Portal	A new link on the My Devices page that lets a user display the personal data stored by Afaria for a selected device. When a user taps the link, the portal displays all stored personal data such as: • User and device data including user name, device serial number, model, and OS • Configuration settings applied to the device through Afaria • The names and versions of the apps installed through Afaria	N/A
Logging	Afaria logs whenever someone accesses views such as list views, custom data views (CDVs), or the device inspector that may display personal user information. This feature allows you to safeguard the personal data of your users by tracking which information has been accessed and by whom. Each INFO log item lists the date and time, the user, and the query used. For standard list views and the inspector, the log lists the query number. For CDVs, the log lists the fields displayed in the view. → Tip We recommend that you clear your logs on a regular basis since this feature can generate many log items.	Server Monitoring

Area	Feature	Documentation Location
Windows and Windows Mobile Clients	In order to comply with the EU's new General Data Protection Regulations, Windows and Windows Mobile users must now accept the End-User License Agreement (EULA) before the client is installed. If the user declines the EULA, the installation of the client is canceled.	N/A

SP27

Area	Feature	Documentation Location
Android Support	Support for Android 8.0 devices. **i Note** Requires the Android client v15567. This version will ship with the Afaria 7 SP28 software. In the meantime, you can download the client from Google Play.	SAP Afaria System Requirements > Device Requirements > Android Devices
iOS Support	Support for iOS 11 devices	SAP Afaria System Requirements > Device Requirements > iOS Devices

SP26

Area	Feature	Documentation Location
Device Management	Admins can now push an app update to iOS devices through the Afaria Admin console by selecting an iOS App Store or Enterprise App policy and clicking the *Repost* button.	SAP Afaria Device Management Guide > Policies
iOS Support	Support for iOS 10.3.3 devices	SAP Afaria System Requirements > Device Requirements > iOS Devices

SP25

Area	Feature	Documentation Location
Inventory	Support for retrieving the MAC address from Android 6.0+ devices for inventory. Security changes from Google required SAP to implement a new method for extracting the device MAC address.	N/A
iOS Support	Support for iOS 10.3.2 devices. Support is no longer available for Apple devices running iOS 6.x or iOS 7.x	SAP Afaria System Requirements > Device Requirements > iOS Devices

SP24

Area	Feature	Documentation Location
iOS Support	Support for iOS 10.3 and 10.3.1 devices.	SAP Afaria System Requirements > Device Requirements > iOS Devices
System Requirements	Support is no longer available for Microsoft SQL Server 2008, Microsoft SQL Server 2008R2, or ASA12. These installations and upgrades will be blocked.	SAP Afaria System Requirements > Database Requirements
System Requirements	Support is no longer available for Windows XP or Windows Server 2003 clients. Any Windows XP or Windows Server 2003 clients or enrollment policies must be deleted prior to upgrading to SAP Afaria 7 SP24.	SAP Afaria System Requirements > Database Requirements
Microsoft .NET Framework Runtime Support	Microsoft .NET Framework Runtime 4.5.1 is no longer supported by Microsoft and therefore is no longer found in the redistributables folder. Microsoft .NET Framework Runtime 4.5.1, 4.5.2, 4.6.1, and 4.6.2 should now be downloaded from Microsoft.	SAP Afaria System Requirements > Installation Image

SP23

Area	Feature	Documentation Location
Windows DM	Windows DM allows the creation of new custom client data view queries.	SAP Afaria Release Notes > Installing and Upgrading SAP Afaria
SMS Gateway	New Cygwin binaries are used in the SMS Gateway.	Installing SAP Afaria > Installing SMS Gateway

SP22

Area	Feature	Documentation Location
Afaria iOS client	The latest iOS client supports App Transport Security (ATS). Apple introduced App Transport Security (ATS) as part of iOS 9.0. ATS is a security feature that improves the privacy and data integrity of connections between an app and web services by enforcing additional security requirements for HTTP-based networking requests. ATS requires iOS 9 or higher devices running these apps to use TLS v1.2 using a server SSL certificate signed with Secure Hash Algorithm 2 (SHA-2) for HTTPS communications. To use this iOS client, configure the servers hosting your Enrollment and Package servers as described in Installing and Upgrading SAP Afaria [page 29]	SAP Afaria System Requirements

SP21

> **i** Important Note
>
> From this release forward, Android for Work will no longer support Google Domain accounts, and will only support Android for Work accounts.
>
> To support Android for Work accounts, the Mobile Secure client must also be updated to the *January client build*. Using an earlier version of the client will result in the failure to inflate the managed profile and the

user's inability to install applications. There is no migration path from Google Accounts to Android for Work accounts: the enterprise must be reenrolled, and clients must also reenroll to use the new account configuration.

Area	Feature	Documentation Location
Afaria client and Self-Service Portal	Support for Croatian.	SAP Afaria System Requirements
Android for Work	Support for Google's new simplified Android for Work enrollment process. With this new enrollment process, you are no longer required to claim the domain or generate tokens and `.p12` files. **i Note** To enroll your enterprise into Android for Work, contact SAP Support for assistance.	Configuring SAP Afaria > Server Configuration for Installation and Management > Android for Work
iOS Support	Support for iOS 10.2.1 devices.	SAP Afaria System Requirements > Device Requirements > iOS Devices
Windows Phone client	The Windows Phone client is now available in Croatian.	N/A

SP20

Area	Feature	Documentation Location
Microsoft .NET Framework Runtime Support	Microsoft .NET Framework Runtime 4.5.1, 4.5.2, 4.6.1, and 4.6.2 are now supported.	SAP Afaria System Requirements
iOS Support	Support for iOS 10.1, 10.1.1, and 10.2 devices.	SAP Afaria System Requirements > Device Requirements > iOS Devices

SP19

Area	Feature	Documentation Location
Windows Support	Support for enrolling Windows Redstone devices	N/A

SP18

Area	Feature	Documentation Location
Android Client	Improvements to the Android 09.2016 client allow users of Samsung KNOX Standard devices (Android 4.3+) to install optional apps from the Android client without having to select “Allow Unknown Sources”. This change provides greater security and improves usability. To take advantage of this functionality, users must re-enroll their devices.	N/A
Android Support	Support for Android 7.0 "Nougat" devices	SAP Afaria System Requirements > Device Requirements > Android Devices
Android for Work	Due to Google's announcement that it will end support for the Android for Work App in Q3 2016, support for this app has been discontinued in this release. The Android for Work App delivers app level containerization of work data to older devices that do not support the Android for Work managed profile. Newer Android devices that support Android for Work natively are not affected. For more information, please refer to the End of Support notice at https://launchpad.support.sap.com/#/notes/2329046	N/A

Area	Feature	Documentation Location
APNs Certificate Support	Updates to support Apple changes to the Apple Push Notification service for both MDM and client APNS Push Certificates. Starting with this release, any new APNs certificate request or renewal will be provisioned from Apple's new sub CA, Apple Application Integration 2 Certification Authority. All client certificates issued by the old sub-CA, Apple Application Integration Certification Authority, will expire on July 26, 2017. Between this release and July 26, 2017, certificates issued from both of these sub CAs will be trusted.	N/A
Device Management	Support for User Certificates with a CA configured for the Entrust protocol on Windows Phone 10 devices.	SAP Afaria Device Management Guide > Policies > Windows Phone Policies > Creating a Configuration Policy > SCEP
	Samsung SAFE is relabelled as Samsung KNOX Standard.	All
	Samsung Enterprise License Model (ELM) is now supported.	SAP Afaria Device Management Guide > Policies > Android Policies > Creating a Configuration Policy for Android > Samsung KNOX Standard Pages
	Updates to the Samsung KNOX Standard Firewall configuration policy to allow administrators to specify deny rules for their firewall.	SAP Afaria Device Management Guide > Policies > Policies > Configuration Policies > Configuration Policies for Android Devices > Samsung KNOX Standard Pages > Firewall Policy
iOS Support	Support for iOS 10, iOS 10.0.1, and iOS 10.0.2 devices.	SAP Afaria System Requirements > Device Requirements > iOS Devices
Samsung SAFE devices	While installing an app from Mobile Place catalog/Afaria client, the *Allow Unknown Sources* prompt which appears has been removed. As an IT administrator, you can create optional application policies in Mobile Place/Afaria such that the app can be updated, unassigned, unpublished or removed without prompting the user.	N/A

SP17

Area	Feature	Documentation Location
System Requirements	Support is no longer available for SAP SQL Anywhere 12.	SAP Afaria System Requirements > Database Requirements
System Requirements	Support is no longer available for Microsoft SQL Server 2008.	SAP Afaria System Requirements > Database Requirements

SP16

Area	Feature	Documentation Location
Device Management	For Windows Phone, an Afaria administrator can send a message to the device after it becomes recompliant.	SAP Afaria Device Management Guide > Device Administration > Defining Remediation Policies for Windows Phone Devices
	For Windows DM, an Afaria administrator can send a message to the device after it becomes recompliant.	SAP Afaria Device Management Guide > Device Administration > Defining Remediation Policies for Windows DM Devices
	An Afaria administrator can track the following certificate details for Windows DM 10: • Date of issue • Issued device • Device to which certificate was issued • Expiry date • Certificate Type (Root/Intermediate) • Common name • Subject alternative name • CA name • Whether CA server supports templates • CA Type (SCEP/Microsoft Native) • Kind of certificate (identity/signing/encrypting) • Revocation details	SAP Afaria Device Management Guide > Device Inspector > Hardware Inventory for Windows DM Devices

Area	Feature	Documentation Location
Mobile Secure for Android client	New Android client, 06.60.10620. This client supports the deployment of optional market apps to Android for Work devices. Users can choose to install the app from the Market page.	N/A
iOS Support	Support for iOS 9.3.3 devices.	SAP Afaria System Requirements > Device Requirements > iOS Devices
Windows support	Windows XP and Windows Server 2003 are no longer supported.	SAP Afaria System Requirements > Device Requirements > Windows Devices

SP15

Area	Feature	Documentation Location
Android support	Android 6.0.1 is now supported.	SAP Afaria System Requirements > Device Requirements > Android Devices
Device Management	New settings in the Android and Android for Work Security policies to allow administrators to disable Smart Lock on Android devices running Lollipop and Marshmallow	SAP Afaria Device Management Guide > Policies > Android Policies > Creating a Configuration Policy for Android Android for Work Quick Start Guide > Creating a Configuration Policy for Android for Work > Security Page
	Removed the ability to use substitution variables for the Entrust Device Type field in the Certificate Authority profile page	Configuring SAP Afaria > Afaria Certificate Management > Creating Certificate Authority Profiles > Entrust Profile Settings

Area	Feature	Documentation Location
	An Afaria administrator can track the following certificate details for Windows Phone: • Date of issue • Issued device • Device to which certificate was issued • Expiry date • Certificate Type (Root/Intermediate) • Common name • Subject alternative name • CA name • Whether CA server supports templates • CA Type (SCEP/Microsoft Native) • Kind of certificate (identity/signing/encrypting) • Revocation details	SAP Afaria Device Management Guide > Device Inspector > Hardware Inventory for Windows Phone Devices
	For Windows DM, an Afaria administrator can send a message to the device after remediation.	SAP Afaria Device Management Guide > Device Administration > Defining Remediation Policies for Windows DM Devices
	Support for User Certificates with a CA configured for the SCEP or SCEP challenge protocol on Windows Phone 8.1 and 10 devices	SAP Afaria Device Management Guide > Policies > Windows Phone Policies > Creating a Configuration Policy > SCEP
	Download the updated version of unsigned Afaria application (.XAP) file for uploading the Application Enrollment Token and Signed Afaria Application.	N/A
Network Access Control Service	The Afaria NAC web service can now be installed on multiple Afaria farm nodes.	SAP Afaria Installation and Configuration Guide > Installing SAP Afaria > Installing Afaria Network Access Control Service

SP14

Area	Feature	Documentation Location
iOS VPP	Starting with iOS9, admins can assign apps to specific devices rather than users. Assigning apps to devices eliminates the requirement for an Apple ID.	SAP Afaria Device Management Guide > Policies > iOS Policies > Volume Purchase Program Licensed Application Policies for iOS Devices > Creating a Volume Purchase Program Licensed App Policy
Android for Work	Admins can now deploy Android market apps as optional apps in the Android for Work managed profile. Users can now view these apps in the Mobile Secure client and choose to install these apps.	Android for Work Quick Start Guide
Certificate Management	Improvements to the handling of identity, MDM, and policy certificates on Android and iOS devices to reduce the number of renewal notifications received by the device.	N/A
Device Management	Support for User Certificates (Microsoft Native) on Windows Phone 8.1 and 10 devices	SAP Afaria Device Management Guide > Policies > Windows Phone Policies > Creating a Configuration Policy > SCEP
System Requirements	Support for IPv6	SAP Afaria System Requirements > SAP Afaria Server Requirements
Certificate Authority Proxy	Install the updated version of CA proxy utility to use the Windows Phone user certificate feature.	N/A

SP13

Area	Feature	Documentation Location
Android Client	The Android client has been rebranded to more closely align with Mobile Secure look and feel, including icon, theme, UI text and versioning.	N/A
iOS Support	Support for iOS 9.2, 9.2.1, 9.3, and 9.3.1 devices	SAP Afaria System Requirements > Device Requirements > iOS Devices

Area	Feature	Documentation Location
iOS Configuration	Support for defining Safari domains in the Per-App VPN payload. You can now list the domains in a per-app VPN profile that you want Safari users to be able to access on your network through VPN.	SAP Afaria Device Management Guide > Policies > iOS Policies > Creating a Configuration Policy for iOS > MDM Payloads > Per-App VPN Payload
iOS Client	The iOS client has been rebranded to more closely align with Mobile Secure look and feel, including icon, theme, UI text and versioning.	N/A
System Requirements	Support for SAP SQL Anywhere 17	SAP Afaria System Requirements > Database Requirements

SP12

Area	Feature	Documentation Location
Android for Work	Afaria automatically and silently pushes updates to apps installed in the Android for Work managed profile when updates are available. If an app's permissions have changed, this is noted in the Server log. To accept new Google productivity app permissions, go to the Google Services page of Server Configuration. For apps installed through an Android Market App policy, open the policy and accept the new permissions.	Android for Work Quick Start Guide
Device Management	Send Message option added on the Device toolbar for Windows Phone	SAP Afaria Device Management Guide > Device Administration > Sending Messages to Devices
	A consolidated Device Model field under *Server* > *Client* in the Device Custom View tool. This data field can be used as a column or to set criteria that will display device models for all device types.	SAP Afaria Device Management Guide > Device Administration > Creating Custom Device Views

Area	Feature	Documentation Location
Windows DM Configuration	Exchange ActiveSync configuration policies support for Windows DM 10	SAP Afaria Device Management Guide > Policies > Windows DM Policies
Windows DM Support	Windows 10 backwards compatibility support for Windows DM devices	SAP Afaria Device Management Guide > Device Enrollment > Windows Device Enrollment

SP11

Area	Feature	Documentation Location
Android for Work	Afaria now automatically and silently pushes Afaria client updates to the Android for Work managed profile. If the Afaria client requires new permissions, this is noted in the Server log. In this case, the admin is required to accept the Afaria client permissions in the *Google Services* page of *Server Configuration*.	Android for Work Quick Start Guide
Windows Support	Users can use remote ring on their Windows Phone 8.1 or Windows Phone 10 devices.	SAP Afaria Device Management Guide > Device Administration > Performing Security Actions on Devices > Security Actions for Windows Devices

SP10

Area	Feature	Documentation Location
Device Management	Support has been removed for Windows device with OS version 8.0.	N/A.
	Administrators can now use directory variables as columns or criteria in custom device views. Admins can also select a device view as the default for the device list.	SAP Afaria Device Management Guide > Device Administration: • Selecting a System or Custom View for the Device List • Creating a Custom Device View
System Requirements	Support for Microsoft SQL Server 2014 Enterprise edition and Standard edition	SAP Afaria System Requirements > Database Requirements

Area	Feature	Documentation Location
	Support has been dropped for Netscape Directory Server and Novell NDS Directory Server	SAP Afaria System Requirements > SAP Afaria Server Requirements

SP9

Area	Feature	Documentation Location
Android for Work	Android for Work can now run on Samsung 5.1.x devices.	N/A
	New procedure to enroll the enterprise as part of the Android for Work setup	Android for Work Quick Start Guide
iOS	Support for iOS 9.1 devices	SAP Afaria System Requirements > Device Requirements > iOS Devices
Device Management	If a user has activated the activation code via EUSSP or Mobile Place without auto discovery, user will not be prompted to enter credentials during enrollment	N/A

SP8

Area	Feature	Documentation Location
Afaria Client	Support for the Serbian language	SAP Afaria System Requirements
Certificate Management	Support for Entrust IdentityGuard certificate authority server versions 8 and 9	Configuring SAP Afaria> Afaria Certificate Management > Entrust Profile Settings
Device Management	Support for VPN on Windows Phone	SAP Afaria Device Management Guide > Policies > Windows Phone Devices > Creating a Configuration Policy > VPN
Self-Service Portal	Support for the Serbian language	SAP Afaria System Requirements
	Gating option allows only approved group members access to the Self-Service Portal.	Configuring SAP Afaria > Configuring Afaria Components > Self-Service Portal

SP7

Area	Feature	Documentation Location
Afaria Client	Support for Czech, Hungarian, and Polish.	SAP Afaria System Requirements
Access Control	Afaria Network Access Control service updated to support Cisco NAC spec version 1.4	N/A

SP6

Area	Feature	Documentation Location
Access Control	Substitution variable support	Configuring SAP Afaria >Access Control>Substitution Variables Examples
Access Control Security Enhancements	• Access control remote multi-CAS support • Access control message handling change	Configuring SAP Afaria > Access Control > Installing Access Control Components on Multiple Machines
Certificate Authority Proxy	CA Proxy installer and service	Configuring SAP Afaria > Access Control > Installing Access Control Components on Multiple Machines > Installing the Filter and the Data Handler Proxy Service Installing SAP Afaria > Upgrading Afaria to SP6 > Upgrade Considerations
Certificate Management	Ability to specify CA for identity certificates	Configuring SAP Afaria > Afaria Certificate Management: • Creating Certificate Authority Profiles • Microsoft CA Profile Settings
	Certificate revocation improvements	
	SCEP policy support for Windows Phone	Configuring SAP Afaria>Afaria Certificate Management>SCEP Profile Settings
Component Installation	Ability to configure database information during installation of the Enrollment Server and Package Server	Installing SAP Afaria

Area	Feature	Documentation Location
Device-Side Certificate Management	In the enrollment policy for Windows XP, Windows Vista, Windows 7, Windows 2003, and Windows Mobile, the device-side certificate location and password are no longer specified as a part of the installation package. Instead, specify the certificate location and password information directly in the Afaria app on the device. [REF SMS-11577]	N/A.
General Security Enhancements	• Disabled XClistener on Afaria server • Resolved CSRF issue • Tenantized the outbound API service to avoid cross-tenant device entries in the message log • Admin and Self-Service Portal session timeout improvements • Poodle vulnerability response - SP5 code base: XSRedirector change to remove CBC cypher suites • iOActive report security improvements • IS Hardening • ERP report security improvements • Standard DB mechanism for password storage • Removed use of blowfish in Windows Phone encryption	N/A
iOS Application Signing	APNs connection management improvements to increase scalability of MDM connections	iOS Application Signing > Afaria Enterprise Client Application > Creating the App ID
iOS Device Inventory	Expanded iOS device hardware inventory	SAP Afaria Device Management Guide > Device Inspector > Hardware Inventory for iOS Devices

Area	Feature	Documentation Location
iOS Device Security	iOS7: Activation lock and clear New managed domains payload Config policy restrictions payload update Per-message email encryption option	SAP Afaria Device Management Guide > Device Administration > Performing Security Actions on Devices > Security Actions for iOS Devices Configuring SAP Afaria > Server Configuration for Installation and Management > Configuring Payload Signing
iOS8 Support	Consent text support	SAP Afaria Device Management Guide > Policies > iOS Policies > Creating an Enrollment Policy for iOS
	DEP terms and conditions message handling	SAP Afaria Device Management Guide > Device Enrollment > iOS Device Enrollment > Apple Device Enrollment Program
	VPN policy support	SAP Afaria Device Management Guide > Policies > iOS Policies > Creating a Configuration Policy for iOS > MDM Payloads: • Per VPN Payload • VPN Payload
iOS9 Support	New support for iOS 9 including the ability to take over management of an unmanaged iOS App Store or Enterprise app without losing user data or having to reinstall the app. When you apply an iOS app policy to a device with the app installed but not managed, the user is prompted to allow management.	SAP Afaria Device Management Guide: • Policies > iOS Policies > Creating an Application Policy for iOS App Store Apps • Device Inspector > Viewing the Device Package Tracking Log
	New settings in restrictions payload	SAP Afaria Device Management Guide > Policies > iOS Policies > Restriction Payload
	WiFi policy update to support EAP as a TTLS inner authentication protocol	SAP Afaria Device Management Guide > Policies > iOS Policies > MDM Payloads > WiFi Payload

Area	Feature	Documentation Location
Network Access Control Security Enhancements	• Support for Windows Phone and Window DM devices • NAC redirect URL tenantization • New calls to return all devices and retrieve a device's application list • Additional device attributes • Run apply policies to force device check-in • NAC compliance attribute increased performance	SAP Afaria System Requirements Configuring SAP Afaria > Configuring Afaria Components: • Support for Network Access Control • Testing the Afaria NAC Service
Windows Phone	Additional commands: Remote Ring, Lock and Reset Pin	SAP Afaria Device Management Guide >Device Administration > Performing Security Actions on Devices > Security Actions for Windows Phone Devices
	Enterprise Assigned Access enables an enterprise to provision a device to a locked-down user experience. The administrator can customize the start screen with pinned applications, control the visibility of certain system settings, and configure custom launch actions for buttons.	SAP Afaria Device Management Guide: • Creating a Configuration Policy for Windows Phone • Assigned Access
	User-initiated unenrollment notification	SAP Afaria Device Management Guide>Device Enrollment > Removing Windows Phone Devices from Management
	Support for non-authenticated enrollment of Windows Phone devices using a Web authentication broker. Requirement for hosting partners who do not have access to end customer's AD.	SAP Afaria Device Management Guide >Device Enrollment > Windows Device Enrollment > Enabling Auto-Discovery for Windows and Windows Phone Devices
	Windows 10 backwards compatibility support for Windows Phone devices	SAP Afaria Device Management Guide > Device Enrollment > Windows Device Enrollment
SAP Afaria Admin Console	New theme for the Admin and Self-Service Portals	N/A
	Improved resolution text for server message logs	N/A

Area	Feature	Documentation Location
System Requirements	Support for: • SAP SQL Anywhere 16 • Windows Server 2012 • Microsoft Active Directory 2012	SAP Afaria System Requirements

3.1 Setting up Apple APNs Certificates for Afaria 7 SP31

Starting with the Afaria 7 SP31 (November 2018) release, Afaria supports Apple's new APNs based on the HTTP/2 network protocol. To use the new APNs, you must upload the appropriate Apple iOS certificates via the Afaria Administration console after installing Afaria 7 SP31.

During the 2018 WWDC conference, Apple announced that the original Apple Push Notification service (APNs) would be deprecated at some future date. EMM/MDM vendors were directed to begin using Apple's new APNs based on the HTTP/2 network protocol.

Afaria uses the APNs to perform the following actions:

- Send MDM push notifications to iOS devices (which are invoked by selecting *Apply Policies* manually or via schedule to push MDM apps and configuration policies)
- Send push notifications/messages to the iOS Afaria app

Upgrade Considerations:

- If you are upgrading from Afaria 7 SP29PL03 (or any one-off patch applied to SP29PL03), you must follow the instructions below to begin using the new APNs after installing Afaria 7 SP31.

If you are upgrading from Afaria 7 SP30:

- If you renewed and/or re-uploaded the Apple certificates listed below after installing Afaria 7 SP30, your system will already be using the new APNs after installing Afaria 7 SP31.
- If you did not renew and/or re-upload the Apple certificates listed below after installing Afaria 7 SP30, you must follow the instructions below to begin using the new APNs after installing Afaria 7 SP31.

3.1.1 Setting up the iOS Apple MDM APNS Certificate

This procedure describes the steps required to set up the iOS Apple MDM APNS Certificate.

Context

Ensure that you have correctly installed Afaria 7 Service Pack 31.

Procedure

1. If the expiration date of your APNs Push Certificate (for Mobile Device Management) is imminent, renew the certificate via Apple's portal as is normally done each year. If your certificate is not expiring soon and you are not ready to renew it, you can use your current iOS Apple MDM APNs Certificate to complete these steps.
2. In the Afaria Administration console, browse to *Server* > *Configuration* > *Component* > *iOS Notification* > *APNs Push Certificate (for Mobile Device Management)*.
3. Upload the *APNs Push Certificate (for Mobile Device Management)*.
4. To verify that the new APNs is in use:
   1. Perform an "Apply Policies" (i.e. send a test web config policy) to a device.
   2. In the Afaria Server Message Log, check for the following entry:
      - `Type: INFO`
      - `Server user: XsQueue.APNS`
      - `Message: APN0050: Push notification success: PushType=MDM, Client=(UDID)FAKEUUIDC2C48638EAEC5E905264D6084A4C0EB0, Endpoint=api.push.apple.com:443`

> **i Note**
>
> The old APNs endpoint was `gateway.push.apple.com:2195`.

3.1.2 Setting up the APNS Push Certificate (for Custom-Signed Afaria Application)

This procedure describes the steps required to set up the APNS Push Certificate (for Custom-Signed Afaria Application).

Context

Ensure that you have correctly installed Afaria 7 Service Pack 31.

Procedure

1. If the expiration date of your APNs Push Certificate (for Custom-Signed Afaria Application) is imminent, renew the certificate via Apple's Developer's tools as is normally done each year. If your certificate is not expiring soon and you are not ready to renew it, you can use your current APNs Push Certificate to complete these steps.
2. In the Afaria Administration console, browse to *Server* > *Configuration* > *Component* > *iOS Notification* > *APNS Push Certificate (for Custom-Signed Afaria Application)*.

3. Upload the *APNS Push Certificate (for Custom-Signed Afaria Application)*.
4. To verify that the new APNs is in use:
    1. Perform a send message/notification to a device via the Afaria console.
    2. In the Afaria Server Message Log, check for the following entry:
        - `Type: INFO`
        - `Server user: XsQueue.APNS`
        - `Message: APN0050: Push notification success: PushType=MDM, Client=(UDID)FAKEUUIDC2C48638EAEC5E905264D6084A4C0EB0, Endpoint=api.push.apple.com:443`

> **i Note**
>
> The old APNs endpoint was `gateway.push.apple.com:2195`.

4 Installing and Upgrading SAP Afaria

Install or upgrade Afaria by downloading the latest version of the Afaria software and run the Afaria `setup` program for each Afaria server and component in your installation.

> **i** Note
>
> When upgrading to the latest version of SAP Afaria, ensure you upgrade all components including the Afaria client.

For more information about installing or upgrading Afaria, refer to the *Installing SAP Afaria* guide.

Installation and Upgrade Considerations

Keep the following in mind when planning to upgrade to or install the latest release of Afaria:

- For Afaria 7 SP28 or later, where the environment is set up for TLS 1.2 only (older security protocols have been disabled), the following registry entries must be set (or created):

  Upgrade a previous version of Afaria to Afaria 7 SP28

  1. Shut down all Afaria services prior to upgrade.
  2. Alter the environment to support TLS 1.2 only (disabling other security protocols).
  3. Set the following registry keys:
     - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Afaria\Afaria]
       "SQLServerDriverOverride"=dword:00000001
     - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
       "SchUseStrongCrypto"=dword:00000001
     - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework
       \v4.0.30319]
       "SchUseStrongCrypto"=dword:00000001
  4. Proceed with the upgrade.

  New installation of Afaria 7 SP28

  1. Before installing Afaria, create the following registry keys:
     - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Afaria\Afaria]
       "SQLServerDriverOverride"=dword:00000001
     - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
       "SchUseStrongCrypto"=dword:00000001
     - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework
       \v4.0.30319]
       "SchUseStrongCrypto"=dword:00000001
  2. Proceed with the installation.
- Windows DM custom client data view queries were corrupted after upgrade to SP19 or later. The problem has been corrected as of SP23, but any defined Windows DM custom queries will need to be manually recreated.

- As a result of the change to the SMS Gateway, when you upgrade to SAP Afaria 7 SP23, the SMS Gateway does not work unless the Cygwin binaries are replaced. In fact, if Afaria is configured to run the SMS Gateway, Afaria no longer starts correctly: an XRS4940 fatal error is generated indicating that an unexpected error has occured in the XSSMSGatewayManager.exe. Until the Cygwin binaries are replaced with the newer versions, this will continue to happen. If Afaria is not configured to use the SMS Gateway, then Afaria starts correctly.
- Starting January 1, 2017, new or updated iOS apps submitted to the Apple App Store require the App Transport Security (ATS) feature. ATS requires iOS 9 or higher devices running these apps to use TLS v1.2 using a server SSL certificate signed with Secure Hash Algorithm 2 (SHA-2) for HTTPS communications. SAP Afaria 7 SP21 includes support for ATS. Before upgrading from SP20 to SP21 or SP22, modify the configurations of the server machines hosting the Afaria enrollment server and package server to use a server SSL certificate signed with SHA-2 and support TLS v1.2 for HTTPS communications. This configuration change can be made in the customer's IIS/Windows servers.
  Please ensure that you make these changes before deploying the latest iOS client as this client includes support for ATS. Once you deploy the latest iOS Client, client communications between iOS 9 or higher devices and an IIS/Windows server not using TLS v1.2 and a server SSL certificate with an SHA-2 signature will fail.

  > **i Note**
  >
  > Moving to SHA-2 and supporting TLS v1.2 should not impact Android or Windows Phone client communications. If Afaria customers are using older versions of Android (Android 4.3 or lower) that don't support TLS v1.2, other TLS versions should be enabled as required.
  >
  > SAP does not claim support for Windows Mobile and/or Windows CE client connections to a server machine hosting an Afaria enrollment server configured to use server SSL certificates signed with SHA-2 and TLS v1.2. To avoid possible impacts, we recommend you set up an additional Afaria enrollment server for use only by Windows Mobile and/or Windows CE clients and configured to use the TLS version and SHA version necessary to maintain support.
- The method of authenticating an outbound notification from the server to a Win32 client on a Vista or newer OS has changed. After a fresh install or an upgrade from a previous release, the client will initiate an encrypted key exchange with the server, and that client will then use the key to authenticate the message is from the correct Afaria server. Outbound to the client will not be possible until the key is exchanged.
  - If the client does not have the key (i.e. fresh install or upgrade), it will request the key from the server on the next connection.
  - If the server does not have the key (i.e. the client was deleted via the admin console, but then later reconnects), then the server will instruct the client to request a new key on the next connection.
  - If the keys get out of synch (i.e. the client was on a VM image that was rolled back to an earlier state prior to a key exchange or database data was restored to an earlier version prior to key exchange), then the client and server can be re-synchronized by deleting the client registry key, deleting the client from the admin console, or deleting the server's encrypted copy the key in the A_ENCRYPTION table, and then having the client reconnect manually or via schedule.

    > **i Note**
    >
    > Deleting the client or the encryption record will require two connections. The first will result in the client being instructed to request a new key, and the second will actually request the key.
- The Android client now correctly reports an Active Sync ID when using the Gmail app as part of Android for Work. This allows Access Control processing to correctly allow or block devices. Customers upgrading from older Android clients will need to re-enroll their Android for Work devices if Gmail is already

configured inside the managed profile. Customers who have not yet deployed Gmail should upgrade to the latest client before doing so to ensure the Active Sync IDs are reported back to Afaria.
Legacy devices that are upgraded to Android for Work will not be included in Access Control processing when using the February 2017 Android client. This means that Nitrodesk and Samsung KNOX Exchange accounts configured outside the managed profile will need to be allowed or blocked at the Exchange server level. After inflating the Android for Work profile, Access Control processing will only apply to the Gmail app inside the managed profile.

4.1 Supported Upgrade Paths

Select the appropriate upgrade path based on your current version of SAP Afaria.

Based on the version of SAP Afaria you are running, do one of the following:

SAP Afaria 7 SP30 or SP31

Upgrade to SAP Afaria 7 SP32.

SAP Afaria 7 SP28 or SP29

1. Upgrade to SAP Afaria 7 SP30.
2. Upgrade to SAP Afaria 7 SP32.

SAP Afaria 7 SP27 or earlier

1. Upgrade to SAP Afaria 7 SP28.
2. Upgrade to SAP Afaria 7 SP30.
3. Upgrade to SAP Afaria 7 SP32.

Supported Android Clients

The following versions of the Android client are supported in this version of SAP Afaria:

- 15998 – Current shipping version
- 15567
- 14742

The best practice is to upgrade your users to the latest client version. Users may skip a version when upgrading the client. For example, users running 14742 may upgrade directly to the current version. Users running older clients need to re-enroll to get the new version.

5 Fixed Issues

Issues fixed in SAP Afaria 7 SP32:

> **Note**
>
> For a list of customer-reported incidents fixed in SP32, refer to the SAP Note at https://launchpad.support.sap.com/#/notes/2731710.

6 Known Issues

Known issues in SAP Afaria at the time of release to the general public.

6.1 Upgrading Afaria

The known issues pertaining to upgrading Afaria are:

- For information about upgrade issues, see the following knowledge base articles and bugs:
  - KBA 2055690
  - KBA 2052429
  - KBA 1900017
  - KBA 2054436
  - KBA 2059434
  - KBA 2059388
- Afaria Server components (Afaria Server, API Server, Enrollment Server, Package Server, and Self-service Portal) now support Windows 2016 Server. However, by default, iOS 11 or higher devices can't enroll successfully: the MDM Token check-in process does not complete and the following error is returned in the Afaria Server Message log:
  `"IPH6034: Token Checkin MDM Message Signing Validation Failure. UDID: xxxxxxxxxxxxxxxxxxxxxxx..."`
  This is a known issue that will be corrected in a future release. As a workaround, the error can be prevented by disabling the HTTP/2 protocol in Windows using the following steps:
  1. Start the Windows Registry Editor.
  2. Navigate to the registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters` and add two new REG_DWORD values:
     - `EnableHttp2Tls = 0`
     - `EnableHttp2Cleartext = 0`
  3. Reboot the machine.
- Afaria needs SQL Anywhere 16 to be patched to a minimum of Express Bug Fix (EBF) 2076 to work without issues. If a more recent EBF, such as 2127, is installed, the .NET framework will need to be updated to version 4.5.1 or later for it to work correctly with Afaria.

6.2 SAP Afaria Server

- Afaria does not currently support Active Directory multi-valued attributes; choose a single-valued attribute when using directory variables in Afaria. If a multi-valued attribute is selected, it is non-deterministic as to which value will be used. [SMS-32472]

- Every time the Afaria client on an Android for Work device connects to the Afaria server, a "Requested to update..." INFO message is logged to the server log. This occurs if the latest available version of an app on Google Play is not supported on the device. This is expected behavior. When the Afaria client connects to the Afaria Server, it compares the installed version of the app with the available version and, if the available version is later, sends a request to update which is logged in an INFO message. If the app cannot be updated, then the process is repeated at the next connection and another message is logged. [SMS-24389]
- Selecting UID as the option for LDAP Security Settings takes longer to authenticate than the cn and samaccountname options. [REF 54321]
- Log on as batch permission is required to communicate with the Certificate Authority if User Account Control is enabled. [REF 54226]
- During the enrollment of Android devices, multiple policy certificate requests are issued for NitroDesk policies. [REF 54591]
- If NitroDesk configuration fails, a new certificate is issued during each Afaria session until the configuration is successful. This is expected behavior. [REF 54600]
- If a user in AD is a member of more than 1000 groups, the user cannot be found. Policy assignments, authentication, requests for directory bindings, and logins to the Afaria Administration console and Self-Service Portal are unsuccessful. [REF Microsoft KB 275266]

6.3 Afaria Administration Console

- The Chrome browser pre-populates password fields in the Afaria Administration console if you set the browser to remember your password when prompted during log in. This is an issue with Chrome. The password is not recognized by Afaria and is not saved to the policy. [REF 51821]
  Workaround: Clear passwords from your browser cache.
- If you filter server logs by Tenant name and then switch to the non-system tenant, the filtering remains in effect. This may lead to no records being displayed until the user removes the filter on the Tenant Name column or the page is refreshed. [REF 54654]

6.4 Self-Service Portal

- Android devices must have cookies enabled in order to use the Self-Service Portal. If cookies are disabled, the device displays a “Server Error in ‘/ssp’ Application” error message.
  Workaround: Enable cookies on the device. [SMS-25489]
- iPad users may be unable to download an Android Enrollment file for an Android device from the Self-Service Portal.
  Workaround: Use a Windows machine for the download or configure and use an online storage app such as Dropbox on your iPad. [REF 53379]
- Users of Android devices running 2.3.x are unable to download an Android Enrollment file using the device's stock browser. The user sees an "Untitled/Download unsuccessful" error message.
  Workaround: Download the enrollment file using a different browser such as Firefox. [REF 53275]

- When re-enrolling Android devices, the Self-Service Portal correctly transitions to the SAP Afaria client but also launches Google Play when users return to the Self-Service Portal with Dolphin and Firefox browsers. [REF 54110]

6.5 Android Devices

- After encryption and reboot on AFW-capable devices, getting a prompt to delete AFW profile and the personal Android client is still present on the device. Following the encryption and rebooting of AFW-capable devices during enrollment into Android for Work, the user is prompted to delete the profile. Inflation of the managed profile continues in the background. After it completes successfully, the personal Android client is still present on the device. [DXSMS-6916]
  Workaround: Do one of the following:
  - After the device reboots after the encryption, wait for the Profile inflation screen to display instead of opening the Android client.
  - Delete the profile and continue with inflation wizard. Select OK to close the error message. Then open the personal Android client and restart the inflation.
- Android 8.0+ (Oreo) includes a new app setting that enables background task throttling. Background task throttling must be set to "OFF" so that the server can execute management commands on the device. The Android client v15567 will only be affected resulting in GCM issues if this setting is enabled by a user. [DXSMS-6648]

  > **i** Note
  >
  > If required, you can reduce the effect of this setting using a remediation policy or an access control policy to enforce connection frequency.

- Pushing Google's Divide Productivity (PIM) apps to an Android 8.0 device causes the Android client to fail and reboot. Divide apps have been retired by Google and are not supported on Android 7 (Nougat) or 8 (Oreo) devices. [DXSMS-6635]
- After the KNOX agent fails during the enrollment of a Samsung KNOX device, the user is not prompted to reboot the device to complete the creation of the Samsung KNOX container. The device displays the following message: "Samsung Knox container creation in progress"; however, the container is never completed. [DXSMS-6025]
  Workaround: Restart the device and re-connect the Android client.
- After configuring a Wi-Fi connection using an Android configuration policy, Wi-Fi SCEP certificates are re-issued on every connection. This occurs if the Wi-Fi policy pushed to the device uses an SSID that has already been configured on the device. [DXSMS-5835]
  Workaround: Remove the Wi-Fi policy creating the duplicate Wi-Fi network and reconnect the Android client.
- With the February 2017 Android client, legacy devices upgraded to Android for Work will not be included in the Access Control processing. Nitrodesk and Samsung KNOX Exchange accounts, configured outside of the managed profile, will need to be allowed or to be blocked at the Exchange Server level. After inflating the Android for Work profile, the Access Control processing will only apply to the Gmail app inside the managed profile. [DXSMS-5095]
- Re-enrollment required for Access Control management with managed Gmail app. If Gmail is already configured inside the managed profile, re-enroll your Android for Work devices. If Gmail has not already

been deployed, upgrade to the most recent Android client version prior to deploying Gmail and this ensures that the Active Sync IDs are reported to Afaria. [DXSMS-5093]

- After applying an Android Security policy to enable SmartLock on Android for Work and Samsung KNOX Standard devices that have activated device admin for exchange account for apps such as Gmail, users are still unable to enable SmartLock. Users receive a message that SmartLock has been disabled by the Device Administrator. [DXSMS-4815]
- The deny firewall rules in the Samsung KNOX Standard configuration policy do not work on the Samsung Galaxy S IV device. This is a Samsung issue. This feature does work on some other Samsung devices. [DXSMS-4561]
- If a user taps the *Home* button on a device during Android for work account profile inflation, the profile inflation window becomes hidden behind the Android client screen and profile inflation cannot continue. [DXSMS-4493]
  Workaround: To continue with profile inflation, either reopen the Android client and tap the *Back* button or reboot the device.
- On Samsung Galaxy S4 mini devices, apps such as the Citrix VPN client cannot find an installed SCEP certificate that they require for authentication. This issue has been observed on S4 devices running the Android client version 11470 and higher. This issue is caused by an issue with the Samsung operating system. For more information on this issue, refer to SAP Knowledge Base article #2437251 at https://launchpad.support.sap.com/#/notes/2437251/E. [DXSMS-2778]
- Android for Work profile inflation fails on the device and the user receives an error message that the Play Store app is out-of-date. [SMS-34088]
  Workaround: Have the user open the Play Store app and update it (*Settings* > *Play Store version*). After the app is updated, Android for Work profile inflation continues.
- Non-Samsung Android devices running 5.1.1 or above always report "False" in the App Running column for software inventory. This is caused by a change by Google to lock down the ability to get the running application data reported in inventory. This issue does not affect Samsung devices running 5.1.1 or above as Samsung still allows access to the running application data reported in inventory. [SMS-33174]
- Android for Work configuration values are not always applied to the badged Android client following enrollment of the device and the inflation of the managed profile. [SMS-33126]
  Workaround: Remove the managed profile and re-enroll the device.
- After a Samsung SAFE device with OS version greater than 4.2 (API level > 17) is upgraded to the September version of the SAP HANA Cloud Platform, mobile service for app and device management client, if MMEP is available and a blacklisted app is installed, the user sees a message `Security policy restricts installation of this application` followed by `<application package> installed`. However, the blacklisted app does not get installed. [REF SMS-32583]
  Workaround: Re-enroll the device and activate ELM.
- After each session following the changing of the password on a Samsung 4.3 or 4.4.2 device, the device reboots and the user receives the following prompt from the Android client: "Certificate installation failed. Lock, then unlock your device." This is a Samsung issue. [SMS-31887]
  Workaround: Apply the latest patches from Samsung. If this does not resolve the issue, clear the “Minimum number of complex characters in password” setting in the Samsung KNOX Standard Password page of the applied Android Configuration policy.
- After a device with OS version greater than 4.2 (API level > 17) is upgraded to the September version of the SAP HANA Cloud Platform, mobile service for app and device management client, if the device has Samsung SAFE device manager policy applied already, then MMEP will not be deleted and the ELM license prompt will not appear.[REF SMS-31683]
  Workaround:
  1. Set *Allow Afaria Device Admin Deactivation* to Yes and apply the device manager policy again.

2. Re-enroll the device using the September version of the SAP HANA Cloud Platform, mobile service for app and device management client. Accept the ELM license.

- When an Android configuration policy for NitroDesk or Exchange Account policy for Android for Work is pushed to an Android 7.0 (N or Nougat) device with the latest client, the configuration fails if the policy includes a static certificate. [SMS-31578]
- The Administrator Lock command does not work on Android 7.0 (N or Nougat) devices in the Device Administrator management mode. After the Admin lock has been applied, the device can still be unlocked by the user using the device passcode. This functionality is still available, from OS 7.0 forward, in the Android For Work Profile Owner management mode and the Android For Work Device Owner management mode. This is the result of changes to Android functionality by Google. [SMS-31539]
- On a Samsung device v 4.3, when collecting inventory data for many installed applications where retrieving the data list of available applications from the OS exceeds the OS limitation of 1 MB, a device reboot occurs. This behavior appears to be specific to this device, but note other device types could exhibit similar behavior if they exceed the OS limitation. [SMS-29768]
- Trusted Face is disabled on an Android for Work device even though Smart Lock is enabled on the device through an Android for Work Security policy. [SMS-29490]
- After an Android for Work device is upgraded to the June version of the Mobile Secure client, the user cannot disable the Smart Lock on the device using an Android for Work Security policy. [SMS-29311]
  Workaround: Remove the managed profile and re-enroll the device.
- Issued certificates are not revoked from an Android for Work device during a remote wipe of the managed profile even if revocation is enabled in the associated Certificate Authority profile. [SMS-29023]
  Workaround: Revoke the certificates manually from the Device list in the Afaria Administration console.
- Android for Work devices require a PIN or better lock if you plan to apply Android for Work policies with embedded certificates. This is a security limitation with Android which requires a lock on the device before it can access the certificate store. If the device doesn't have a lock set, any applied policies with embedded certificates will fail. [SMS-28984]
- If an attempt to install an Android for Work optional app fails, no error message is displayed. The App Info page in the Mobile Secure client indicates that app installation is progress but the app is not successfully downloaded nor installed. [SMS-28524]
  Workaround: Retry the installation at a later time.
- Following an upgrade to Afaria 7 SP15, the *Smart Lock disabled* radio buttons on a configured Android for Work Security page (password settings enabled) are disabled. [SMS-28131]
  Workaround: To enable the Smart Lock settings on an existing policy, clear and then re-select the *Enable Password* check box at the top of the Android for Work Security page.
- Smart Lock is still disabled on a Samsung Galaxy S6, SM-G920A device running Android 5.1.1 even after a applying an Android configuration policy with Smart Lock disabled set to “No” in the Android Security policy page. This issue is also observed after applying this setting from the Security policy page of an Android for Work configuration policy. This is a Samsung issue and has been fixed in later builds of Samsung software. [SMS-28239]
- The application icon for Android for Work optional apps do not display correctly in the Mobile Secure client on the managed profile. Please note that the icon does display properly in the Android app policy on the Afaria Admin console. [SMS-27783]
- Android devices must have cookies enabled in order to use the Self-Service Portal. If cookies are disabled, the device displays a “Server Error in ‘/ssp’ Application” error message.
  Workaround: Enable cookies on the device. [SMS-25489]
- Every time the Afaria client on an Android for Work device connects to the Afaria server, a "Requested to update..." INFO message is logged to the server log. This occurs if the latest available version of an app on Google Play is not supported on the device. This is expected behavior. When the Afaria client connects to

the Afaria Server, it compares the installed version of the app with the available version and, if the available version is later, sends a request to update which is logged in an INFO message. If the app cannot be updated, then the process is repeated at the next connection and another message is logged. [SMS-24389]

- Android 6.0 Marshmallow, Power-Saving Optimization option Doze - When an Android 6.0 Marshmallow device goes into the Doze mode, inbound schedules will no longer run until the user wakes the device. This design minimizes the battery usage when the device is idle. As a side effect, the schedules will only run when the user wakes the device. A plugged in device does not experience this issue, since plugging in a device prevents it from entering the Doze mode. A recovery mechanism for the Android 6.0 Marshmallow Doze mode now exists which runs schedules in the next maintenance window. [SMS-20935]
- Following the enrollment of an Android device, the enrollment file (.eaef file) is not deleted if the user saves the file to their external SD card. [SMS-18821]
- Session policies fail to send a file to an external SD card on an Android 4.0 and above device. Any attempt to send a file to an external SD card results in a "SYS0005: Access is denied" error in the server connection log. This is caused by a Google security restriction on Android KitKat and above devices. [SMS-18229]
- Android for Work devices do not report all device activity such as incoming messaging data and voice data for device activity collection. Please note that Afaria does not support device activity on Android for Work devices. [SMS-17824]
- Camera does not launch for devices running KNOX container 2.0 even if the restriction policy is set to 'Camera Enable'. This behavior is observed when the camera option is disabled in the 'Configuration Policy' for Android and 'Restriction Policy' for Samsung SAFE. This is an issue with Samsung API. [SMS-17097]
- Disabled Android for Work configuration policies are applied to a device during re-enrollment if the policy has not been unpublished or unlinked. During re-enrollment, the work profile is created even though the policy is disabled. Once a configuration policy is made Android for Work, it cannot be reverted to a legacy policy.
  Workaround: Unpublish the configuration policy and then re-enroll the device. [SMS-15823]
- If an Enterprise Google user is logged into personal Google play before enrollment, then Enterprise apps are available to install until the user logs out from Google Play. This is a Google issue. [SMS-13402]
- During enrollment, the user receives a number of Android for Work prompts if an Android for Work policy is applied and Device Activity Collection is enabled. During enrollment, the device connects multiple times to execute device activity collection. On each connection, the user receives a "Press OK to begin AW configuration" prompt followed by multiple notifications as well as a prompt to remove the profile, "You already have a work profile on your device. Do you want to remove it?" [SMS-12402]
  Workaround: If you enable Device Activity Collection, do not assign any Android for Work policies until the initial device activity collection is complete.
- While the Afaria client is connected to the Afaria server, Samsung SAFE device users can change device settings even if "Allow Settings Changes" in the Samsung SAFE Restrictions policy is set to "No". [SMS-9380]
- Session policies are not supported on Android for Work devices. [SMS-8130]
- Application policy failed to disable an application (make the app icon invisible inside the container) in KNOX 1.0 container.
- During enrollment of a Samsung SAFE device with an installed AES2 client, the client switches to the base/MMEP application but does not present an activation screen for the Afaria client.
  Workaround: Enable device admin on the Afaria client or re-enroll the device. [REF 54684]
- A certificate on an Android device may not renew during the certificate renewal window. This can occur if multiple Android devices with certificates connect simultaneously for renewals. The certificate should renew during the next renewal window. [REF 54675]

- The Afaria Samsung AES2 Client available from the Google Play store is not supported on Android KitKat devices. [REF 54672]
- On Samsung devices, it is possible that the Afaria MMEP file will be sent to the device multiple times. [REF 54662]
- Re-enrolling Android devices issues new SSO certificates consistently, but EAS certificates only intermittently. Re-enrolling does not issue new NitroDesk, Wi-Fi, or SCEP certificates. Clearing data issues all new certificates, but EAS certificates only intermittently. [REF 54618]
- Intermittent issues when installing applications from Google Play Store. Problems may include Google Play Store or the device crashing. This is an issue with Google Play Store. [REF 54589]
- Unable to create an Exchange account on a Samsung S3/ICS device using a Samsung Exchange account policy if a prior attempt to create the account failed because of invalid settings.
  Workaround: Remove the Email address value from the EAS account in the policy and reapply it to the device; then re-add the Email address value and reapply the policy to the device. [REF 54556]
- The Samsung Email Account configuration policy creates a duplicate email account on Android KitKat devices on subsequent sessions. This occurs if the incoming and outgoing user names are not in the format `<username>@<domain>`. KitKat devices require this format. [REF 54457]
- The Android Enrollment file fails to download from the Self-Service Portal if the user uses either Chrome or a native browser and the Self-Service Portal uses HTTPS. This issue is caused by an issue with the Android Download Manager. Refer to issue 3492 on the Android Open Source Project - Issue Tracker site for more information.
  Workaround: Use Firefox to enroll the device or return to the Self-Service Portal and tap *Launch and Enroll* again. [REF 54001]
- For Samsung Galaxy S5 devices, the Exchange - ActiveSync Device ID reported in Afaria Inventory does not match the ID in the default mail client in the Samsung KNOX container. This is an issue with Samsung KNOX. [REF 53961]
- Certificates cannot be installed in Samsung KNOX containers before version 2.0 using an Afaria Samsung KNOX certificate policy. Users of the Samsung device will receive an error message that KNOX security policies restrict the installation of certificates. This is working as designed by Samsung.

  > **i Note**
  >
  > Samsung KNOX 2.0 does not have this restriction. Samsung devices with KNOX 2.0 - such as the Samsung S5 - are allowed to install certificates through KNOX. [REF 53939]

- Android 4.2 and later devices will not connect successfully over SSL if the certificate has been signed with an MD5 signature. This is a security restriction of Android 4.2+ devices. [REF 53914]
- If inventory is deleted for an Android device from the *Devices* page of the Afaria Administration console, the device does not receive policies during the next session and the user receives a message that "Certificate failed authentication. Try reset credentials, enroll again or contact your administrator".
  Workaround: Reset credentials or re-enroll the device. [REF 53910]
- If a user deactivates the Afaria Samsung MMEP application from the *Device administrators* page of a Samsung device, they can bypass policies and restrictions previously applied to the device.
  Workaround: Create and deploy a Device Manager policy (*Android Configuration* > *Samsung SAFE* > *Device Manager Policy*) with *Allow Afaria Device Admin Deactivation* set to "No". [REF 53909]
- Users can uninstall an application even when uninstallation is disabled in a Samsung SAFE Application configuration policy if the same application is set as optional in an Android Enterprise Application policy. If you create a Samsung policy for an application with installation and uninstallation settings, do not create a separate Android Enterprise Application policy for the application. [REF 53908]

- Commands sent from Afaria via SMS are not deleted from Android 4.4 following execution. These messages remain in the SMS inbox and are visible to the end-user. This is a known restriction with 4.4 (KitKat). Changes to SMS notifications introduced by Google prevent apps from aborting the SMS_RECEIVED_ACTION broadcast. The Afaria client cannot delete the message before it is received and displayed by the user's SMS app. [REF 53681]
- Users enrolling Android devices through the Self-Service Portal may see a message such as "This content is unsupported content. Do you really want to download?" when downloading the Android enrollment file. This enrollment file contains configuration details for enrolling with Afaria and uses an `.eaef` extension. This extension may not be recognized by native browsers on some Android devices. It is safe to tap *Download* and continue with enrollment. [REF 53390]
- Following an Afaria Server upgrade to SP5, you cannot remove a Wi-Fi SSID from a device using the Samsung Wi-Fi configuration policy if the device is running a pre-SP5 version of the Afaria client application.
  Workaround: Upgrade the client to SP5. [REF 52690]
- An Android device's user value format changes from `<user>` to `<domain>\<exchangeID>` when the Afaria client is launched for the first time. This occurs for Android devices with NitroDesk installed that have been manually enrolled. This behavior is by design. When the device enrolls, a UserID is supplied and displayed in the *User* column of the *Device* list. When the client is launched for the first time, this value changes to the `<domain>\<exchangeID>` format. This does not occur for devices enrolled through the Self-Service Portal. [REF 52256]
- When a device action such as Lock Device or Apply Administrator Lock is sent to an Android KitKat device, the device displays the command as a text message. Afaria uses SMS for outbound notifications including security actions. The action is performed on the device but a text message is also displayed. This is known behavior with KitKat devices. [REF 51927]
- Application shortcuts are not added to the Home screen of the Samsung KNOX container during container creation. If you configure a Samsung KNOX configuration policy to add a shortcut and apply this policy to a device without Samsung KNOX installed, then Afaria initiates the creation of the KNOX container but the shortcut is not added until the next connection with Afaria. This is a known issue with pre-2.0 versions of Samsung KNOX. [REF 51683]
- Outbound notifications sent by Afaria are not received on some Android devices because the phone number/SMS address used is missing the required country code. Afaria retrieves the phone number as formatted on the device. On some devices, the phone number does not include the country code.
  Workaround: From the Afaria Administration console, add the country code to the SMS address field on the *Device* > *Edit* page for the device. [REF 48680]

6.6 iOS Devices

- If an iOS user attempts to install a VPP optional app from the iOS client immediately after enrolling into VPP, the app is pushed to the device but may not be installed. [SMS-34106]
  Workaround: The user should tap *Install* again from the iOS client.
- The data displayed for Ratings Region and Restrictions for Movies & TV shows are incorrect due to the 'Ratings region' not being returned when an iOS device is queried. Because each Ratings region has its own set of values for Movies and TV shows, the Ratings Region must be known in order to display the value returned by the device for Movies and TV Shows. This is why the raw (non-interpreted) value for the setting is displayed in the Device Inspector view. Changes made to the Movies and TV Shows settings in the

Restrictions Configuration Policy are reflected on the device but the associated Ratings region remains set to the value of 'United States'. [Apple Bug 27643725, SMS-30296, BCP 133580]

- App Store apps deployed using an iOS App Store policy with “Deploy using MDM protocol” enabled are not pushed to devices running iOS 9.3.2 to 9.3.5. An error message, “IPH3011: iOS[12023] The iTunes Store ID of the application could not be validated”, appears in the server log. This is a known Apple issue and is caused if the app is not already in the purchase history associated with the user’s Apple ID. This issue has been fixed in iOS 10.
  Please refer to SAP KBA #2338214 at https://launchpad.support.sap.com/#/notes/2338214 for more information. [Apple bug 27112311, SMS-30367, SMS-30912, BCP 231459]
  Workaround: Customers that must deploy App Store apps and cannot wait for a fix from Apple can create a new iOS App Store policy to distribute the app, but ensure that the “Deploy using MDM protocol” check box on the *General* page is **not** enabled. Note that this app will therefore not be an MDM-managed or controlled app.
- Passcode Required prompt continuously disappears and reappears after an iOS 9 device without a passcode receives a configuration payload requiring a passcode. This is a known issue with iOS 9.
  Workaround: Set a passcode on the device before enrollment. If you encounter this issue during enrollment, restart the device, set the passcode, and then continue with the enrollment process. [Apple bug 22976156, SMS-20547]
- iOS VPN payloads with SSL (Custom) connection type are not delivered to the iOS device. This is a known issue with iOS. [SMS-18543]
- The deletion of an iOS device’s hardware inventory causes existing certificates to be revoked and new certificates to be re-issued when you next apply policies to the device. [SMS-10496]
- Due to issues in the NitroDesk TouchDown application (V3.1.0 available in App Store), the iOS NitroDesk Calendar settings 'Work Day Start' and 'Work Day End' are not configured correctly, when the TouchDown application is configured through the Afaria 7 SP4 application. This issue has to be addressed by NitroDesk. [REF 51381]
- The Apply Configuration and Skip Configuration options do not appear on the Apple Device Enrollment Program configuration screen. [REF Apple bug 16404559]
  Workaround: Click *Back* and then return to the screen to make the options appear.
- The Apple Device Enrollment Program does not support the use of user prompts (configured on the variable tab) in enrollment policies. If an enrollment policy includes user prompts, the user prompts are ignored. [REF 53062]
- The Apple Device Enrollment Program is not compatible with other existing enrollment flows in SAP Afaria, including the Self-Service Portal. [REF 53062]
  Workaround: To use the Self-Service Portal with the Apple Device Enrollment Program, manually enter the Self-Service Portal registered user in the iOS device record in SAP Afaria.
- The Apple Device Enrollment Program uses the same deferred delivery process for MDM required application polices as it uses for configuration policies with supervised payloads. This is to work around the Apple bug that executes the Apple Device Enrollment Program during setup but does not manage the prompting for installation of MDM required application policies for the remainder of the setup. This prevents the prompts from appearing. [REF Apple bug 16430116]
- The Apple Device Enrollment profile setting for the *Skip Location Services* setup panel does not work when using the cellular network on the device for setup. [REF Apple bug 16558155]
- The apply configuration functionality of the Apple Device Enrollment Program on devices intermittently returns the error message: "The configuration for your iPhone could not be downloaded from <CompanyName>. The request timed out." The issue seems to be related to connectivity or performance issues with the Apple Cloud server from which the device retrieves the Apple Device Enrollment Profile. This issue occurs approximately 5 times per 50 enrollments. [REF Apple bug 16657457]
  Workaround: Go back a screen and select *Apply Configuration* again a few seconds later.

- If the Install prompt for the MDM application policy push is displayed when the device auto locks, unlocking the device dismisses the Install prompt and prevents the installation of the application. [REF Apple bug 16657452]
- Choosing Skip the Configuration during activation of a device that is associated with an Apple Device Enrollment Program account applies the Supervised setting of the DEP payload. [REF Apple bug 17826636]
  Workaround: Disassociate the device from the DEP profile and perform a hard reset.
- iOS client enrollments using an MDM enrollment URL receive a 'ClientDAL.RunQuery: Cannot convert to a uniqueidentifier' error. [REF CSS 0120061532/0001496697/2014]
- The ICCID system variable for iOS devices is not populated, so it cannot be resolved in policies. [REF 52385]

6.7 Windows Phone Devices

- Windows Phone enrollment fails in a farm environment with multiple enrollment servers due to a MAC validation failure. ASP.NET automatically generates a cryptographic key for each application and stores the key in the HKCU registry hive. This auto-generated key is used if there is no explicit `<machineKey>` element in the application's configuration. However, because this auto-generated key is local to the computer that created the key, this scenario causes a problem for applications that run in a farm.
  Workaround: Do one of the following:
  - Create an explicit `<machineKey>` element to the application's Web.config file in the AIPSR subfolder of the Enrollment Server directory. This enables the auto-generated cryptographic key to be overridden by the machine key added in `Web.config` file.
  - Enable affinity in the load balancer

  For more information, refer to KBA 2292594 at https://launchpad.support.sap.com/#/notes/2292594.
- App restriction policy does not work as expected on Windows Phone with OS version 10. [REF SMS-24023]
- Unable to enroll Windows phone with OS version 8.10.12393.890 from Mobile Place portal. [REF SMS-23734]
  Workaround: To enroll Windows phone from Mobile Place portal, ensure to upgrade your OS to 8.10.14219.341 and later.
- While working Windows devices with OS version 10 with assigned access:
  - Disabling System Settings such as Data Sense, Date and Time, and VPN are supported
  - Disabling Application Settings is not supported

  [REF SMS-18099]

6.8 Windows Devices

- Unlinking the Windows 8.1 (Windows DM) configuration policy from a device does not delete the certificate from the device.
  Workaround: The user should manually delete the certificate. [REF 54034]

- In the Windows DM configuration policy SCEP details page, if you edit any of the fields and save the policy, a duplicate certificate is pushed to the device.
  Workaround: The user should manually delete the duplicate certificate. [REF 54033]
- Device actions such as lock device, apply policies, and unenroll device need Windows Push Notification service support. Push notifications will not work on Windows 8.1 devices if the scheduled tasks, namely MDMAppInstallationTask or MDMMaintenanceTask, are running.[REF SMS-31347, 53948]
  Workaround: End the MDMAppInstallationTask or the MDMMaintenanceTask, if device action commands are not working from either the Admin UI or from the Self-Service Portal.
- On requesting a DM sync, deletion of multiple VPN profiles from the windows phone device is not supported. Only one VPN profile gets deleted on every DM sync. This is Microsoft issue. [REF SMS- 20209]
- In the Windows DM Configuration Policy, if Passcode Policy is configured, the passcode settings are not enforced immediately. There could be a delay of about eight hours before these settings are applied on the device. This behavior is observed on Windows DM with OS version 8.1. [REF 53960].

7 Afaria Product Variables

This topic holds all the variables created for the product SAP Afaria.

product-name-registered SAP Afaria
product-name-nonregistered SAP Afaria
product-name-short Afaria
company-name SAP
admin-interface-name Afaria Administration console
portal-name Self-Service Portal

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.

www.sap.com/contactsap

THE BEST RUN SAP